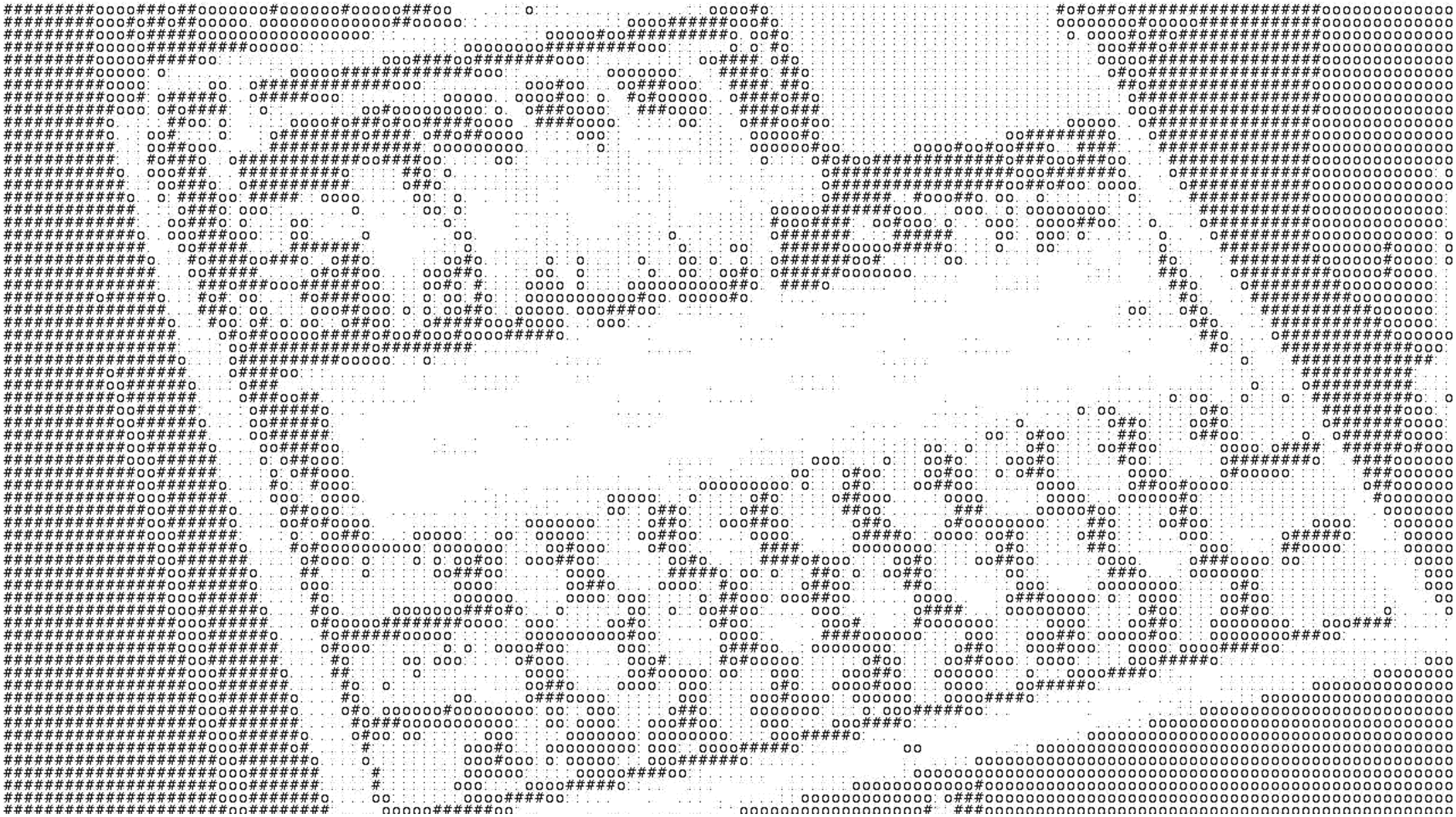


The ASCII Enigma Cryptographic Protocol (AECP) | John Robert Bruhling | March 13, 2019

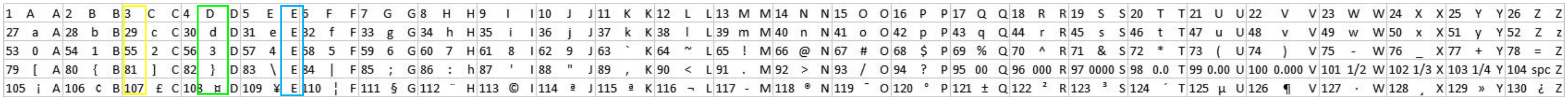
The ASCII Enigma Cryptographic Protocol or AECP is designed to encode common messages into an enigma machine compatible format with a degree of encryption. The mechanism encodes/decodes 130 common ASCII characters from a variable Master Character field which is then randomized and continuously shifted throughout the entire process. This process is governed by two other fields of which are determined by similar measures. For a single ASCII character, 3-4 letters of a random order are ascribed. These letters are subject to a variable shift and salting prior to being passed through a string of 5 Enigma machines where each letter passes through a variable path. These outputs (and enigma machines) are also subject to a variable salting and shift. All of these parameters are defined in the Master Key set which describes the initial setup and expected functions. A system of seeding is used to describe the various shifting. These unique shifting functions rely on linear causality and exact pairing of an indeterminate key size. The testing of this protocol called for 5 separate enigma machine simulators and some fancy spreadsheet work. The programs used are called "Enigma Simulator" and "WPS spreadsheet".

https://play.google.com/store/apps/details?id=uk.co.franklinheath.enigmasim

http://wiki.franklinheath.co.uk/index.php/Enigma/Simulator_User_Guide

https://www.wps.com/spreadsheets

The operator might first begin the initial setup by selecting the master character field. The one used for this example is arbitrary incorporating common characters found on a keyboard as well as a few odd ones. A programmable implementation could use different ASCII characters and a front-end app could correlate many different character sets to those. (The Master Key set is of an arbitrary format decided on for compact size and is described below).



1	A	A	2	B	B	3	C	C	4	D	D	5	E	E	6	F	F	7	G	G	8	H	H	9	I	I	10	J	J	11	K	K	12	L	L	13	M	M	14	N	N	15	O	O	16	P	P	17	Q	Q	18	R	R	19	S	S	20	T	T	21	U	U	22	V	V	23	W	W	24	X	X	25	Y	Y	26	Z	Z
27	a	A	28	b	B	29	c	C	30	d	D	31	e	E	32	f	F	33	g	G	34	h	H	35	i	I	36	j	J	37	k	K	38	l	L	39	m	M	40	n	N	41	o	O	42	p	P	43	q	Q	44	r	R	45	s	S	46	t	T	47	u	U	48	v	V	49	w	W	50	x	X	51	y	Y	52	Z	z
53	0	A	54	1	B	55	2	C	56	3	D	57	4	E	58	5	F	59	6	G	60	7	H	61	8	I	62	9	J	63	`	K	64	~	L	65	!	M	66	@	N	67	#	O	68	$	P	69	%	Q	70	^	R	71	&	S	72	*	T	73	(	U	74	)	V	75	-	W	76	_	X	77	+	Y	78	=	Z
79	[	A	80	{	B	81	]	C	82	}	D	83	\	E	84	|	F	85	;	G	86	:	h	87	'	I	88	"	J	89	,	K	90	<	L	91	.	M	92	>	N	93	/	O	94	?	P	95	00	Q	96	000	R	97	0000	S	98	0.0	T	99	0.00	U	100	0.000	V	101	1/2	W	102	1/3	X	103	1/4	Y	104	spc	Z
105	¡	A	106	¢	B	107	£	C	108	¤	D	109	¥	E	110	¦	F	111	§	G	112	¨	H	113	©	I	114	ª	J	115	ª	K	116	¬	L	117	-	M	118	®	N	119	¯	O	120	°	P	121	±	Q	122	²	R	123	³	S	124	´	T	125	µ	U	126	¶	V	127	·	W	128	¸	X	129	»	Y	130	¿	Z

Each cell contains a number, character and a letter pointer. The number associates the character to a referenced cell and the pointer is location specific to its current placement on the field.

The key format for this protocol is described below. For brevity this example will be applied to our description.

1) B-C-Y.B6.C3.D8-1J.2U.3G.4Q-AR-YTVW/
2) A0-T-14532.SCFEP.K/
3) C-B3.C3.D1-1H.2D.3O.4Y-AA-RCVN/

4) A-31245.JKYVX.E/
5) C-B3.C1.D2-1G.2V.3W.4I-UU-YTER/
6) D-EOEO-V-F-WHTL-11-FI
7) A-A-A4.B2.C7-1Q.2C.3J-ZX-RNR/
8) C-B3.C1.D3-1K.2F.3Y.4V-FF-HGYN/
9) B-B-Y.B7.C2.D5-1I.2F.3G.4U-SE-FFXN/
10) B-C-B.B4.C3.D7-1N.2H.3L.4S-VM-IJKA/
11) C-B1.C1.D2-1G.2M.3N.4R-OO-YFOQ/
12) 0.G4.7/3.Y1.3/1.N1.0/
13) 0.4.2.-2.3.6/1.2.1-5.8.0/

Row 1 - 1st Enigma key to derive the pointer field (explained below) (B-C-Y.B6.C3.D8-1J.2U.3G.4Q-RA-YTVW/)

Row 2 - Master Character field reference (designated volume A, chapter 0)

- Pointer field pointer generator reference (a random letter placed at the beginning of the field reference to be passed through the first vending machine , T)
- row placement (the order of the rows versus their original placement ,14352)
- Pointer field key (determines the alignment of the columns vertically by their pointers, SCFEP)
- Home position (designated by the pointer in row 1 set to cell A1 of the Hard row, K)

Row 3 - 2nd Enigma key to derive Shifter field (C-B3.C3.D1-1H.2D.3O.4Y-AA-RCVN/)

Row 4 - Shifter field generator reference (like the Pointer field generator reference, will be assigned for the second Enigma machine and Shifter field , A)

- row placement (31245)
- Shifter field key (vertical column key by pointers, JKYVX)
- Home position (designated by the pointer in row 1 set to the Hard row cell A1, E)

Row 5 - 3rd Enigma key for Salt field (C-B3.C1.D2-1G.2V.3W.4I-UU-YTER/)

Row 6 - Phasic salt generator reference (like the previous generator references, will be assigned to the salt field, D)

- Phasic salt EO seed (determines if and where Phasic salt will occur, is referenced from the numeric equivalency of even or odd of the letters of the pre encrypted Cipher text, EOEO)

- Slide seed generator reference (generator reference for the Slider field, V)

- Slide seed (determines how a Slide function will execute ,F)

- Height seed (determines the paths through which the pointers will pass through the 5 Enigma machines, WHTL)

- Phasic salt percentage (determines how many of the Phasic salt EO seeds will apply Phasic salt , 11)

- Salt field key (sets the Salt Field by their pointers, FI)

Row 7-11 - Enigma keys (×5) for final encryption
Machine 1) A-A-A4.B2.C7-1Q.2C.3J-ZX-RNR/
2) C-B3.C1.D3-1K.2F.3Y.4V-FF-HGYN/
3) B-B-Y.B7.C2.D5-1I.2F.3G.4U-SE-FFXN/
4) B-C-B.B4.C3.D7-1N.2H.3L.4S-VM-IJKA/
5) C-B1.C1.D2-1G.2M.3N.4R-OO-YFOQ/

Row 12- Polyphasic salt parameters (determines how and when Polyphasic salt will occur , 0.G4.7/3.Y1.3/1.N1.0/)

Row 13 - Phantom shift parameters (determines how and when a Phantom shift will occur , 0.4.2.-2.3.6/1.2.1-5.8.0/)

(Keys are forward slash delineated, macros are hyphen delineated and individual variables are period delineated.)

The Enigma keys are formatted as; B-C-Y.B6.C3.D8-1J.2U.3G.4Q-AR-YTVW/

Machine type -
A) M3 1939
B) M4 1942
C) K Railway

Reflector type for machine-
A) A, B, C
B) B, C
C) no value (ommited)

Wheel number 1-8 for machine-

A) A1-8, B1-8, C1-8

B) (B or Y),B1-8, C1-8, D1-8

Ring settings for machine-

A) 1A-Z, 2A-Z, 3A-Z

B) 1A-Z, 2A-Z, 3A-Z, 4A-Z

C) 1A-Z, 2A-Z, 3A-Z, 4A-Z

C) (A= no value) B1-8, C1-8, D1-8

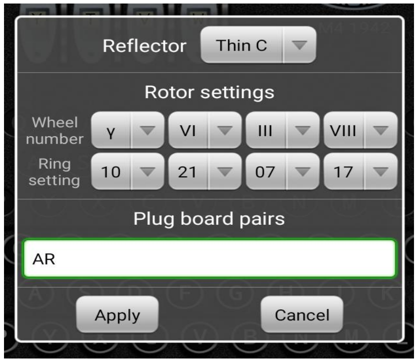
Plug board pairs A-Z+A-Z (If no value substitute one self pair such as AA)

Counter settings (external rotor) A-Z for machine -

A) A-Z, A-Z, A-Z

B) A-Z, A-Z, A-Z, A-Z

C) A-Z, A-Z, A-Z, A-Z

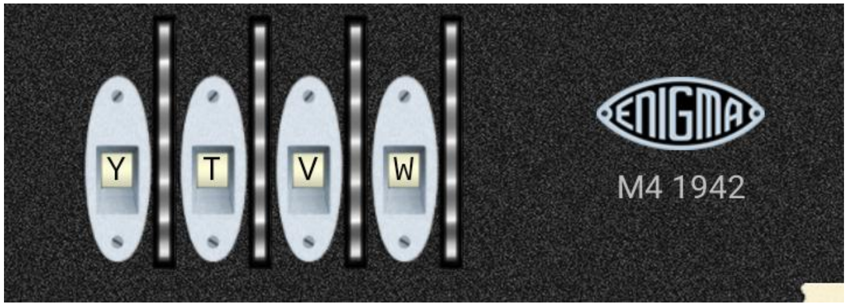

Reflector: Thin C

Rotor settings

Wheel number: Y, VI, III, VIII

Ring setting: 10, 21, 07, 17

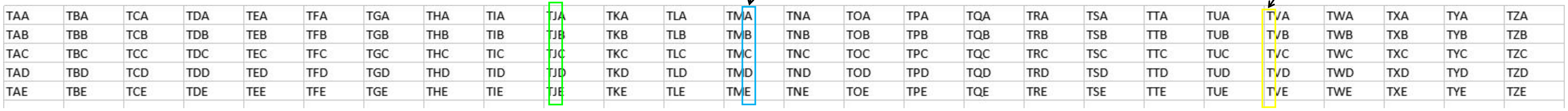
Plug board pairs: AR



The Pointer and Shifter field format is 5 rows of 26 cells, 4 rows of 16 for the Salt field and 1 row of 6 for the Slider row).

The operator determines a Pointer field reference generator (A-Z). We then assign for each cell a unique 3 lettered set consisting of the Pointer generator reference and 2 field position references; 1 for the column A-Z and 1 for the row A-Z in that order.

A0-T-14532.SCFEP.K/



TAA	TBA	TCA	TDA	TEA	TFA	TGA	THA	TIA	TJA	TKA	TLA	TMA	TNA	TOA	TPA	TQA	TRA	TSA	TTA	TUA	TVA	TWA	TXA	TYA	TZA
TAB	TBB	TCB	TDB	TEB	TFB	TGB	THB	TIB	TJB	TKB	TLB	TMB	TNB	TOB	TPB	TQB	TRB	TSB	TTB	TUB	TVB	TWB	TXB	TYB	TZB
TAC	TBC	TCC	TDC	TEC	TFC	TGC	THC	TIC	TJC	TKC	TLC	TMC	TNC	TOC	TPC	TQC	TRC	TSC	TTC	TUC	TVC	TWC	TXC	TYC	TZC
TAD	TBD	TCD	TDD	TED	TFD	TGD	THD	TID	TJD	TKD	TLD	TMD	TND	TOD	TPD	TQD	TRD	TSD	TTD	TUD	TVD	TWD	TXD	TYD	TZD
TAE	TBE	TCE	TDE	TEE	TFE	TGE	THE	TIE	TJE	TKE	TLE	TME	TNE	TOE	TPE	TQE	TRE	TSE	TTE	TUE	TVE	TWE	TXE	TYE	TZE

We set the first Enigma machine key that will be used and pass the 130 cell references through this Enigma machine B-C-Y.B6.C3.D8-1J.2U.3G.4Q-AR-YTVW/

EHG	UOP	CPW	CHU	CRZ	RPE	EZI	FJJ	HAY	WPB	UFG	FTP	ELF	WBD	YWL	RIM	IYO	RDQ	WQO	GYV	CAG	GOR	LSC	WBW	YDF	YAH
DWH	CYM	SPA	HZD	PRY	OBI	NOI	OGT	OGF	XGK	WRI	SEG	VEC	CKK	SPI	OFC	SDI	LLJ	PMF	OAD	MWR	MUL	GIG	GVK	QWZ	XLH
APV	DIX	FBG	GZE	PMI	BGS	SXF	VLD	LWF	ESZ	CGJ	IRO	XAZ	FTO	FNI	GNA	DAF	JHO	RKG	VYF	YGS	LRQ	MZB	ARN	GJK	PSD
VOH	USB	QEX	QIR	NHN	FKV	ONU	JBJ	PRG	KEQ	YWW	CAF	PSI	YBA	ISK	ZRH	XJW	BNN	DLS	RKI	LKJ	BWC	EZR	CFH	AFU	KMK
NJJ	HEP	PAI	KYX	LVU	QVJ	POK	VLA	POX	AIP	JVP	DQJ	KIJ	BWF	INR	VCO	DSP	ADT	WPI	XWK	ISI	PZR	WTH	WJX	KEK	PAD

and derive the above references.

We then rearrange these 130 outputs in alphabetical order,

ADT	AFU	AIP	APV	ARN	BGS	BNN	BWC	BWF	CAF	CAG	CFH	CGJ	CHU	CKK	CPW	CRZ	CYM	DAF	DIX	DLS	DQJ	DSP	DWH	EHG	ELF
ESZ	EZI	EZR	FBG	FJJ	FKV	FNI	FTO	FTP	GIG	GJK	GNA	GOR	GVK	GYV	GZE	HAY	HEP	HZD	INR	IRO	ISI	ISK	IYO	JBJ	JHO
JVP	KEK	KEQ	KIJ	KMK	KYX	LKJ	LLJ	LRQ	LSC	LVU	LWF	MUL	MWR	MZB	NHN	NJJ	NOI	OAD	OBI	OFC	OGF	OGT	ONU	PAD	PAI
PMF	PMI	POK	POX	PRG	PRY	PSD	PSI	PZR	QEX	QIR	QVJ	QWZ	RDQ	RIM	RKG	RKI	RPE	SDI	SEG	SPA	SPI	SXF	UFG	UOP	USB
VCO	VEC	VLA	VLD	VOH	VYF	WBD	WBW	WJX	WPB	WPI	WQO	WRI	WTH	XAZ	XGK	XJW	XLH	XWK	YAH	YBA	YDF	YGS	YWL	YWW	ZRH

assign the number and character associated with that encrypted output to its new position and assign to each cell A through Z in order.

122 ² A	103 1/4 B	114 ª C	53 0 D	76 _ E	58 5 F	96 000 G	100 0.000 H	118 ® I	90 < J	21 U K	102 1/3 L	63 ` M	4 D N	40 n O	3 C P	5 E Q	28 b R	69 % S	54 1 T	97 0000 U	116 ¬ V	121 ± W	27 a X	1 A Y	13 M Z
62 9 A	7 G B	101 1/2 C	55 2 D	8 H E	84 | F	67 # G	66 @ H	12 L I	49 w J	77 + K	68 $ L	22 V M	50 x N	20 T O	56 3 P	9 I Q	106 ¢ R	30 d S	119 ¯ T	64 ~ U	125 µ V	93 / W	17 Q X	86 : Y	70 ^ Z
115 « A	129 » B	88 " C	117 - D	104 "sp" E	108 ¤ F	99 0.00 G	44 r H	74) I	23 W J	109 ¥ K	61 8 L	48 v M	47 u N	75 - O	83 \ P	105 ¡ Q	33 g R	46 t S	32 f T	42 p U	35 i V	34 h W	85 ; X	130 ¿ Y	107 £ Z
45 s A	57 4 B	111 § C	113 © D	87 ' E	31 e F	78 = G	91 . H	126 ¶ I	81] J	82 } K	110 ¦ L	51 y M	18 R N	16 P O	71 & P	98 0.0 Q	6 F R	43 q S	38 l T	29 c U	41 o V	59 6 W	11 K X	2 B Y	80 { Z
120 ° A	39 m B	112 ¨ C	60 7 D	79 [E	72 * F	14 N G	24 X H	128 ¸ I	10 J J	123 ³ K	19 S L	37 k M	127 · N	65 ! O	36 j P	95 00 Q	52 z R	124 ´ S	26 Z T	92 > U	25 Y V	73 (W	15 0 X	89 , Y	94 ? Z

We then choose each rows new position. A0-T-14532.SCFEP.K/

122 ² A	103 1/4 B	114 ª C	53 0 D	76 _ E	58 5 F	96 000 G	100 0.000 H	118 ® I	90 < J	21 U K	102 1/3 L	63 ` M	4 D N	40 n O	3 C P	5 E Q	28 b R	69 % S	54 1 T	97 0000 U	116 ¬ V	121 ± W	27 a X	1 A Y	13 M Z
45 s A	57 4 B	111 § C	113 © D	87 ' E	31 e F	78 = G	91 . H	126 ¶ I	81] J	82 } K	110 ¦ L	51 y M	18 R N	16 P O	71 & P	98 0.0 Q	6 F R	43 q S	38 l T	29 c U	41 o V	59 6 W	11 K X	2 B Y	80 { Z
120 ° A	39 m B	112 ¨ C	60 7 D	79 [E	72 * F	14 N G	24 X H	128 ¸ I	10 J J	123 ³ K	19 S L	37 k M	127 · N	65 ! O	36 j P	95 00 Q	52 z R	124 ´ S	26 Z T	92 > U	25 Y V	73 (W	15 0 X	89 , Y	94 ? Z
115 « A	129 » B	88 " C	117 - D	104 "sp" E	108 ¤ F	99 0.00 G	44 r H	74) I	23 W J	109 ¥ K	61 8 L	48 v M	47 u N	75 - O	83 \ P	105 ¡ Q	33 g R	46 t S	32 f T	42 p U	35 i V	34 h W	85 ; X	130 ¿ Y	107 £ Z
62 9 A	7 G B	101 1/2 C	55 2 D	8 H E	84 | F	67 # G	66 @ H	12 L I	49 w J	77 + K	68 $ L	22 V M	50 x N	20 T O	56 3 P	9 I Q	106 ¢ R	30 d S	119 ¯ T	64 ~ U	125 µ V	93 / W	17 Q X	86 : Y	70 ^ Z

We set the Pointer field key by the pointers. A0-T-14532.SCFEP.K/

122 ² A	103 1/4 B	114 ª C	53 0 D	76 _ E	58 5 F	96 000 G	100 0.000 H	118 ® I	90 < J	21 U K	102 1/3 L	63 ` M	4 D N	40 n O	3 C P	5 E Q	28 b R	69 % S	54 1 T	97 0000 U	116 ¬ V	121 ± W	27 a X	1 A Y	13 M Z
82 } K	110 ¦ L	51 y M	18 R N	16 P O	71 & P	98 0.0 Q	6 F R	43 q S	38 l T	29 c U	41 o V	59 6 W	11 K X	2 B Y	80 { Z	45 s A	57 4 B	111 § C	113 © D	87 ' E	31 e F	78 = G	91 . H	126 ¶ I	81] J
127 · N	65 ! O	36 j P	95 00 Q	52 z R	124 ´ S	26 Z T	92 > U	25 Y V	73 (W	15 0 X	89 , Y	94 ? Z	120 ° A	39 m B	112 ¨ C	60 7 D	79 [E	72 * F	14 N G	24 X H	128 ¸ I	10 J J	123 ³ K	19 S L	37 k M
48 v M	47 u N	75 - O	83 \ P	105 ¡ Q	33 g R	46 t S	32 f T	42 p U	35 i V	34 h W	85 ; X	130 ¿ Y	107 £ Z	115 « A	129 » B	88 " C	117 - D	104 "sp" E	108 ¤ F	99 0.00 G	44 r H	74) I	23 W J	109 ¥ K	61 8 L
17 Q X	86 : Y	70 ^ Z	62 9 A	7 G B	101 1/2 C	55 2 D	8 H E	84 | F	67 # G	66 @ H	12 L I	49 w J	77 + K	68 $ L	22 V M	50 x N	20 T O	56 3 P	9 I Q	106 ¢ R	30 d S	119 ¯ T	64 ~ U	125 µ V	93 / W

We then set the Home position to cell A of the Hard row. This is a set row which designates the columns A-Z used by the shifting functions (all shifting happens against this row). Also represented is an E or O to quick reference even or odd. The Pointer field is now set. A0-T-14532.SCFEP.K/

A		O	B		E	C		O	D		E	E		O	F		E	G		O	H		E	I		O	J		E	K		O	L		E	M		O
21	H	K	102	1/3	L	63	`	M	4	D	N	40	n	O	3	C	P	5	E	Q	28	b	R	69	%	S	54	1	T	97	0000	U	116	¬	V	121	±	W
29	c	U	41	o	V	59	6	W	11	K	X	2	B	Y	80	{	Z	45	s	A	57	4	B	111	§	C	113	©	D	87	'	E	31	e	F	78	=	G
15	0	X	89	,	Y	94	?	Z	120	°	A	39	m	B	112	¨	C	60	7	D	79	[	E	72	*	F	14	N	G	24	X	H	128	¸	I	10	J	J
34	h	W	85	;	X	130	¿	Y	107	£	Z	115	«	A	129	»	B	88	"	C	117	-	D	104	"sp"	E	108	¤	F	99	0.00	G	44	r	H	74	)	I
66	@	H	12	L	I	49	w	J	77	+	K	68	$	L	22	V	M	50	x	N	20	T	O	56	3	P	9	I	Q	106	¢	R	30	d	S	119	¯	T

N		E	O		O	P		E	Q		O	R		E	S		O	T		E	U		O	V		E	W		O		X	E	Y		O	Z		E
27	a	X	1	A	Y	13	M	Z	122	²	A	103	1/4	B	114	ª	C	53	0	D	76	_	E	58	5	F	96	000	G	100	0.000	H	118	®	I	90	<	J
91	.	H	126	¶	I	81	]	J	82	}	K	110	¦	L	51	y	M	18	R	N	16	P	O	71	&	P	98	0.0	Q	6	F	R	43	q	S	38	l	T
123	³	K	19	S	L	37	k	M	127	·	N	65	!	O	36	j	P	95	00	Q	52	z	R	124	´	S	26	Z	T	92	>	U	25	Y	V	73	(	W
23	W	J	109	¥	K	61	8	L	48	v	M	47	u	N	75	-	O	83	\	P	105	¡	Q	33	g	R	46	t	S	32	f	T	42	p	U	35	i	V
64	~	U	125	u	V	93	/	W	17	Q	X	86	:	Y	70	^	Z	62	9	A	7	G	B	101	1/2	C	55	2	D	8	H	E	84	|	F	67	#	G

We then perform a similar task for the Shifter field which is where we will derive all of the shift correlations used throughout the protocol. It contains 1) the correlation row, 2) 1st conversion row, 3) 2nd conversion row, 4) spaces row and 5) direction row. Below is the Master Shifter field reference. Unlike the Pointer field, the number is free of the character and the character is row specific. The pointers are assigned in the same A-Z manner and continuing the row references.

1	A	A	2	B	B	3	C	C	4	D	D	5	E	E	6	F	F	7	G	G	8	H	H	9	I	I	10	J	J	11	K	K	12	L	L	13	M	M
27	A	A	28	B	B	29	C	C	30	D	D	31	E	E	32	F	F	33	G	G	34	H	H	35	I	I	36	J	J	37	K	K	38	L	L	39	M	M
53	A	A	54	B	B	55	C	C	56	D	D	57	E	E	58	F	F	59	G	G	60	H	H	61	I	I	62	J	J	63	K	K	64	L	L	65	M	M
79	1 (1)	A	80	2 (2)	B	81	3 (3)	C	82	4 (4)	D	83	5 (5)	E	84	6 (1)	F	85	7 (2)	G	86	8 (3)	H	87	9 (4)	I	88	10 (5)	J	89	11 (1)	K	90	12 (2)	L	91	13 (3)	M
105	L	A	106	R	B	107	L	C	108	R	D	109	L	E	110	R	F	111	L	G	112	R	H	113	L	I	114	R	J	115	L	K	116	R	L	117	L	M

14	N	N	15	O	O	16	P	P	17	Q	Q	18	R	R	19	S	S	20	T	T	21	U	U	22	V	V	23	W	W	24	X	X	25	Y	Y	26	Z	Z
40	N	N	41	O	O	42	P	P	43	Q	Q	44	R	R	45	S	S	46	T	T	47	U	U	48	V	V	49		WW	50	X	X	51	Y	Y	52	Z	Z
66	N	N	67	O	O	68	P	P	69	Q	Q	70	R	R	71	S	S	72	T	T	73	U	U	74	V	V	75	W	W	76	X	X	77	Y	Y	78	Z	Z
92	14 (4)	N	93	15 (5)	O	94	16 (1)	P	95	17 (2)	Q	96	18 (3)	R	97	19 (4)	S	98	20 (5)	T	99	21 (1)	U	100	22 (2)	V	101	23 (3)	W	102	24 (4)	X	103	25 (5)	Y	104	26 (3)	Z
118	R	N	119	L	O	120	R	P	121	L	Q	122	R	R	123	L	S	124	R	T	125	L	U	126	R	M	127	L	W	128	R	X	129	L	Y	130	R	Z

The operator assigns a Shifter generator reference. A-31245.JKYVX.E/

AAF	ABF	ACF	ADF	AEF	AFF	AGF	AHF	AIF	AJF	AKF	ALF	AMF	ANF	AOF	APF	AQF	ARF	ASF	ATF	AUF	AVF	AWF	AXF	AYF	AZF
AAG	ABG	ACG	ADG	AEG	AFG	AGG	AHG	AIG	AJG	AKG	ALG	AMG	ANG	AOG	APG	AQG	ARG	ASG	ATG	AUG	AVG	AWG	AXG	AYG	AZG
AAH	ABH	ACH	ADH	AEH	AFH	AGH	AHH	AIH	AJH	AKH	ALH	AMH	ANH	AOH	APH	AQH	ARH	ASH	ATH	AUH	AVH	AWH	AXH	AYH	AZH
AAI	ABI	ACI	ADI	AEI	AFI	AGI	AHI	AII	AJI	AKI	ALI	AMI	ANI	AOI	API	AQI	ARI	ASI	ATI	AUI	AVI	AWI	AXI	AYI	AZI
AAJ	ABJ	ACJ	ADJ	AEJ	AFJ	AGJ	AHJ	AIJ	AJJ	AKJ	ALJ	AMJ	ANJ	AOJ	APJ	AQJ	ASJ	ASJ	ATJ	AUJ	AVJ	AWJ	AXJ	AYJ	AZJ

A second Enigma machine key is set and the 130 cell references are passed through the Enigma machine. C-B3.C3.D1-1H.2D.3O.4Y-AA-RCVN/

YPX	FVM	XYT	EUT	IXJ	KTY	DSJ	KZW	GNJ	FHI	UGV	LAU	OUN	LHT	DQR	TGQ	LJZ	EJN	UCK	GEG	WCG	YIG	NUB	UTP	LNB	ISP
OKM	MNU	OMA	YGV	CHK	VUI	TPV	JWS	QUH	NDP	JSO	HJJ	MTE	QAJ	ZPY	JXU	GLX	OMF	EHI	IEY	NNC	SXY	NKH	EMS	WEM	SDS
WOZ	TVA	IXD	DAF	OJU	QHT	GCT	KKC	CAQ	DFC	FIG	FCN	XIY	IGZ	MKT	NSD	IJS	MOU	GBJ	YHK	EEQ	GUJ	EUY	SOS	KFM	XYO
TVX	VFG	GGO	NLD	FRO	WIK	UUA	HEU	BJG	JRG	HJG	VUX	QOW	GLL	LXL	VNM	QFM	WBW	QEP	RUS	OPY	WYH	YPZ	DKJ	HDE	JOD
OND	JCI	PUU	CGT	ETI	XVK	ISI	BTH	WGB	TVN	OOA	CBF	NAA	OBC	JTV	SZI	RFW	IDP	EMZ	WFD	KWR	PPG	KKV	RLR	FTH	YWT

Subsequently, the 130 outputs are rearranged alphabetically

BJG	BTH	CAQ	CBF	CGT	CHK	DAF	DFC	DKJ	DQR	DSJ	EEQ	EHI	EJN	EMS	EMZ	ETI	EUT	EUY	FCN	FHI	FIG	FRO	FTH	FVM	GBJ
GCT	GEG	GGO	GLL	GLX	GNJ	GUJ	HDE	HEU	HJG	HJJ	IDP	IEY	IGZ	IJS	ISI	ISP	IXD	IXJ	JCI	JOD	JRG	JSO	JTV	JWS	JXU
KFM	KKC	KKV	KTY	KWR	KZW	LAU	LHT	LJZ	LNB	LXL	MKT	MNU	MOU	MTE	NAA	NDP	NKH	NLD	NNC	NSD	NUB	OBC	OJU	OKM	OMA
OMF	OND	OOA	OPY	OUN	PPG	PUU	QAJ	QEP	QFM	QHT	QOW	QUH	RFW	RLR	RUS	SDS	SOS	SXY	SZI	TGQ	TPV	TVA	TVN	TVX	UCK
UGV	UTP	UUA	VFG	VNM	VUI	VUX	WBW	WCG	WEM	WFD	WGB	WIK	WOZ	WYH	XIY	XVK	XYO	XYT	YGV	YHK	YIG	YPX	YPZ	YWT	ZPY

and the number associated with each encrypted output is placed in its new cell position.

87	112	61	116	108	31	56	62	102	15	7	73	45	18	50	123	109	4	75	64	10	63	83	129	2	71
59	20	81	92	43	9	74	103	86	89	38	122	46	66	69	111	26	55	5	106	104	88	37	119	34	42
77	60	127	6	125	8	12	14	17	25	93	67	28	70	39	117	36	49	82	47	68	23	118	57	27	29
44	105	115	99	13	126	107	40	97	95	58	91	35	121	128	98	52	76	48	120	16	33	54	114	79	19
11	24	85	80	94	32	90	96	21	51	124	113	84	53	100	65	110	78	3	30	72	22	1	101	130	41

We place the rows in their new positions. A-31245.JKYVX.E/

77	60	127	6	125	8	12	14	17	25	93	67	28	70	39	117	36	49	82	47	68	23	118	57	27	29
87	112	61	116	108	31	56	62	102	15	7	73	45	18	50	123	109	4	75	64	10	63	83	129	2	71
59	20	81	92	43	9	74	103	86	89	38	122	46	66	69	111	26	55	5	106	104	88	37	119	34	42
44	105	115	99	13	126	107	40	97	95	58	91	35	121	128	98	52	76	48	120	16	33	54	114	79	19
11	24	85	80	94	32	90	96	21	51	124	113	84	53	100	65	110	78	3	30	72	22	1	101	130	41

Then, for the **original encrypted letter output** (above), we rearrange alphabetically by row.

CAQ	DAF	DFC	EEQ	EUY	FCN	FIG	GBJ	GCT	GUJ	IGZ	IJS	IXD	KFM	KKC	MKT	MOU	NSD	OJU	QHT	SOS	TVA	WOZ	XIY	XYO	YHK
DQR	DSJ	EJN	EUT	FHI	FVM	GEG	GNJ	ISP	IXJ	KTY	KZW	LAU	LHT	LJZ	LNB	NUB	OUN	TGQ	UCK	UGV	UTP	WCG	XYT	YIG	YPX
CHK	EHI	EMS	GLX	HJJ	IEY	JSO	JWS	JXU	MNU	MTE	NDP	NKH	NNC	OKM	OMA	OMF	QAJ	QUH	SDS	SXY	TPV	VUI	WEM	YGV	ZPY
BJG	DKJ	FRO	GGO	GLL	HDE	HEU	HJG	JOD	JRG	LXL	NLD	OPY	QEP	QFM	QOW	RUS	TVX	UUA	VFG	VNM	VUX	WBW	WIK	WYH	YPZ
BTH	CBF	CGT	EMZ	ETI	FTH	IDP	ISI	JCI	JTV	KKV	KWR	NAA	OBC	OND	OOA	PPG	PUU	RFW	RLR	SZI	TVN	WFD	WGB	XVK	YWT

We assign each cell their new characters referenced by row from the Master Shifter field and their pointers A-Z.

77 I A	60 D B	127 J C	6 U D	125 W E	8 L F	12 K G	14 S H	17 G I	25 V J	93 N K	67 Q L	28 C M	70 Y N	39 H O	117 O P	36 R Q	49 P R	82 E S	47 F T	68 X U	23 B V	118 A W	57 M X	27 Z Y	29 T Z
87 O A	112 G B	61 R C	116 D D	108 J E	31 B F	56 T G	62 I H	102 Z I	15 E J	7 F K	73 H L	45 L M	18 N N	50 Q O	123 Y P	109 W Q	4 M R	75 P S	64 S T	10 K U	63 X V	83 U W	129 C X	2 V Y	71 A Z
59 E A	20 S B	81 X C	92 Q D	43 L E	9 T F	74 K G	103 H H	86 P I	89 B J	38 M K	122 J L	46 W M	66 T N	69 A O	111 C P	26 R Q	55 N R	5 I S	106 Z T	104 V U	88 G V	37 F W	119 Y X	34 D Y	42 O Z
44 9 (4) A	105 24 (4) B	115 5 (5) C	99 3 (3) D	13 14 (4) E	126 25 (5) F	107 8 (3) G	40 11 (1) H	97 26 (1) I	95 10 (5) J	58 15 (5) K	91 4 (4) L	35 21 (1) M	121 19 (4) N	128 17 (2) O	98 13 (3) P	52 20 (5) Q	76 1 (1) R	48 7 (2) S	120 2 (2) T	16 16 (1) U	33 12 (2) V	54 18 (3) W	114 6 (1) X	79 22 (2) Y	19 23 (3) Z
11 R A	24 R B	85 R C	80 L D	94 L E	32 L F	90 R G	96 L H	21 R I	51 L J	124 L K	113 L L	84 L M	53 R N	100 L O	65 L P	110 R Q	78 L R	3 L S	30 R T	72 R U	22 R V	1 R W	101 L X	130 R Y	41 R Z

We set the Shifter field key A-31245.JKYVX.E/

77 I A	60 D B	127 J C	6 U D	125 W E	8 L F	12 K G	14 S H	17 G I	25 V J	93 N K	67 Q L	28 C M	70 Y N	39 H O	117 O P	36 R Q	49 P R	82 E S	47 F T	68 X U	23 B V	118 A W	57 M X	27 Z Y	29 T Z
112 G B	61 R C	116 D D	108 J E	31 B F	56 T G	62 I H	102 Z I	15 E J	7 F K	73 H L	45 L M	18 N N	50 Q O	123 Y P	109 W Q	4 M R	75 P S	64 S T	10 K U	63 X V	83 U W	129 C X	2 V Y	71 A Z	87 O A
111 C P	26 R Q	55 N R	5 I S	106 Z T	104 V U	88 G V	37 F W	119 Y X	34 D Y	42 O Z	59 E A	20 S B	81 X C	92 Q D	43 L E	9 T F	74 K G	103 H H	86 P I	89 B J	38 M K	122 J L	46 W M	66 T N	69 A O
35 21 (1) M	121 19 (4) N	128 17 (2) O	98 13 (3) P	52 20 (5) Q	76 1 (1) R	48 7 (2) S	120 2 (2) T	16 16 (1) U	33 12 (2) V	54 18 (3) W	114 6 (1) X	79 22 (2) Y	19 23 (3) Z	44 9 (4) A	105 24 (4) B	115 5 (5) C	99 3 (3) D	13 14 (4) E	126 25 (5) F	107 8 (3) G	40 11 (1) H	97 26 (1) I	95 10 (5) J	58 15 (5) K	91 4 (4) L
100 L O	65 L P	110 R Q	78 L R	3 L S	30 R T	72 R U	22 R V	1 R W	101 L X	130 R Y	41 R Z	11 R A	24 R B	85 R C	80 L D	94 L E	32 L F	90 R G	96 L H	21 R I	51 L J	124 L K	113 L L	84 L M	53 R N

and then set the Home position against the Hard row A cell. The Shifter field is now set. A-31245.JKYVX.E/

A O	B E	C O	D E	E O	F E	G O	H E	I O	J E	K O	L E	M O	N E	O O	P E	Q O	R E	S O	T E	U O	V E	W O	X E	Y O	Z E
125 W E	8 L F	12 K G	14 S H	17 G I	25 V J	93 N K	67 Q L	28 C M	70 Y N	39 H O	117 O P	36 R Q	49 P R	82 E S	47 F T	68 X U	23 B V	118 A W	57 M X	27 Z Y	29 T Z	77 I A	60 D B	127 J C	6 U D
31 B F	56 T G	62 I H	102 Z I	15 E J	7 F K	73 H L	45 L M	18 N N	50 Q O	123 Y P	109 W Q	4 M R	75 P S	64 S T	10 K U	63 X V	83 U W	129 C X	2 V Y	71 A Z	87 O A	112 G B	61 R C	116 D D	108 J E
106 Z T	104 V U	88 G V	37 F W	119 Y X	34 D Y	42 O Z	59 E A	20 S B	81 X C	92 Q D	43 L E	9 T F	74 K G	103 H H	86 P I	89 B J	38 M K	122 J L	46 W M	66 T N	69 A O	111 C P	26 R Q	55 N R	5 I S
52 20 (5) Q	76 1 (1) R	48 7 (2) S	120 2 (2) T	16 16 (1) U	33 12 (2) V	54 18 (3) W	114 6 (1) X	79 22 (2) Y	19 23 (3) Z	44 9 (4) A	105 24 (4) B	115 5 (5) C	99 3 (3) D	13 14 (4) E	126 25 (5) F	107 8 (3) G	40 11 (1) H	97 26 (1) I	95 10 (5) J	58 15 (5) K	91 4 (4) L	35 21 (1) M	121 19 (4) N	128 17 (2) O	98 13 (3) P
3 L S	30 R T	72 R U	22 R V	1 R W	101 L X	130 R Y	41 R Z	11 R A	24 R B	85 R C	80 L D	94 L E	32 L F	90 R G	96 L H	21 R I	51 L J	124 L K	113 L L	84 L M	53 R N	100 L O	65 L P	110 R Q	78 L R

Next, we set the Salt field. We first assign the Salt field generator references, set the 3rd enigma key and pass the following lines

D-EOEO-V-F-WHTL-11-FI C-B3.C1.D2-1G.2V.3W.4I-UU-YTER/

DAK	DBK	DCK	DDK	DEK	DFK	DGK	DHK	DIK	DJK	DKK	DLK	DMK	DNK	DOK	DPK
DAL	DBL	DCL	DDL	DEL	DFL	DGL	DHL	DIL	DJL	DKL	DLL	DML	DNL	DOL	DPL
VAM	VBM	VCM	VDM	VEM	VFM										

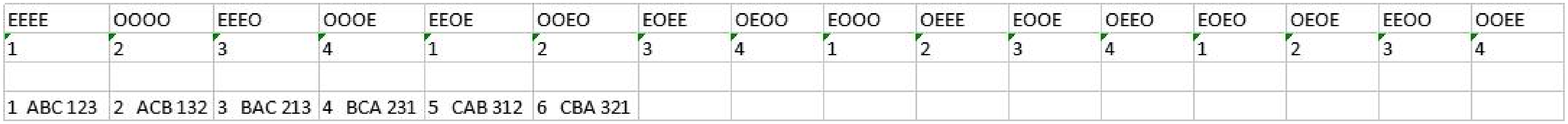
to obtain the outputs.

LVQ	HHN	ZMO	IYJ	JZE	NWS	ZYH	MKO	TKC	XOD	AGZ	TRN	QDA	WCS	VHH	SZM
EWI	YAX	HEJ	QRX	WHX	VUY	KTH	IQQ	SJE	FWV	WGU	VBU	OSD	RKB	KYS	GJI
OYT	CAA	OSH	YYW	MHU	DJE										

We rearrange these outputs alphabetically by their rows,

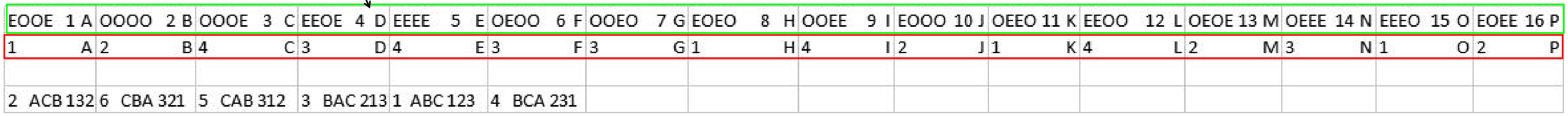
AGZ	HHN	IYJ	JZE	LVQ	MKO	NWS	QDA	SZM	TKC	TRN	VHH	WCS	XOD	ZMO	ZYH
EWI	FWV	GJI	HEJ	IQQ	KTH	KYS	OSD	QRX	RKB	SJE	VBU	VUY	WGU	WHX	YAX
CAA	DJE	MHU	OSH	OYT	YYW										

and reference the characters from the Master Salt field



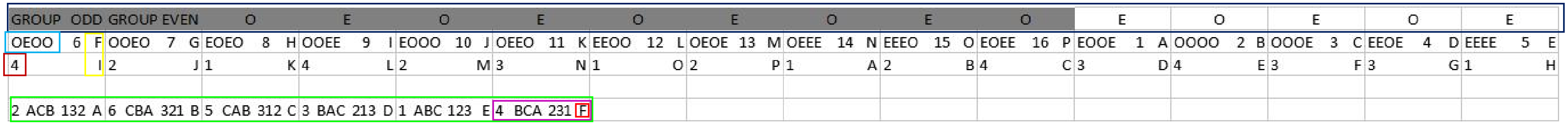
EEEE	OOOO	EEEO	OOOE	EEOE	OOEO	EOEE	OEOO	EOOO	OEEE	EOOE	OEEO	EOEO	OEOE	EEOO	OOEE
1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1 ABC 123	2 ACB 132	3 BAC 213	4 BCA 231	5 CAB 312	6 CBA 321										

to their new positions. We assign A-P in order for the Phasic salt row and EO position row.



EOOE 1 A	OOOO 2 B	OOOE 3 C	EEOE 4 D	EEEE 5 E	OEOO 6 F	OOEO 7 G	EOEO 8 H	OOEE 9 I	EOOO 10 J	OEEO 11 K	EEOO 12 L	OEOE 13 M	OEEE 14 N	EEEO 15 O	EOEE 16 P
1 A	2 B	4 C	3 D	4 E	3 F	3 G	1 H	4 I	2 J	1 K	4 L	2 M	3 N	1 O	2 P
2 ACB 132	6 CBA 321	5 CAB 312	3 BAC 213	1 ABC 123	4 BCA 231										

We set the Salt field key and Phasic salt percentage. Represented in the EO group row as a fraction of 16 (shaded area, 11), it correlates the active salting functions. The Slider row, EO group and EO position rows are not changeable past the initial setup. The Salt field is now set. D-EOEO-V-F-WHTL-11-FI



GROUP ODD	GROUP EVEN	O	E	O	E	O	E	O	E	O	E	O	E	O	E
OEOO 6 F	OOEO 7 G	EOEO 8 H	OOEE 9 I	EOOO 10 J	OEEO 11 K	EEOO 12 L	OEOE 13 M	OEEE 14 N	EEEO 15 O	EOEE 16 P	EOOE 1 A	OOOO 2 B	OOOE 3 C	EEOE 4 D	EEEE 5 E
4 I	2 J	1 K	4 L	2 M	3 N	1 O	2 P	1 A	2 B	4 C	3 D	4 E	3 F	3 G	1 H
2 ACB 132 A	6 CBA 321 B	5 CAB 312 C	3 BAC 213 D	1 ABC 123 E	4 BCA 231 F										

The Slider row designates how the pointers are shifted prior to Phasic salting by referencing how the pointer arrangement changes from ABC 123.There are 6 implementations. The Slide seed being F points to BCA 231 so the first pointer moves to the last position and a new seed reference is taken from the numeric equivalency of the letters (A=1, B=2..) and their respective height within the group. This new seed is referenced for the next permutation.

There are 16 implementations and 4 positions for Phasic salting. Referred to as EO seed they are a variable preset. [note: the E's and O's in the EO group row are placeholders and will not be referenced.]

↑A↑B↑C↑

Positions 1 2 3 4

We then assign the five individual Enigma machine Keys which will be used for final encryption.

A-A-A4.B2.C7-1Q.2C.3J-ZX-RNR/
C-B3.C1.D3-1K.2F.3Y.4V-FF-HGYN/
B-B-Y.B7.C2.D5-1I.2F.3G.4U-SE-FFXN/
B-C-B.B4.C3.D7-1N.2H.3L.4S-VM-IJKA/
C-B1.C1.D2-1G.2M.3N.4R-OO-YFOQ/

We then assign Polyphasic salt parameters and Phantom shift parameters.

0.G4.7/3.Y1.3/1.N1.0/

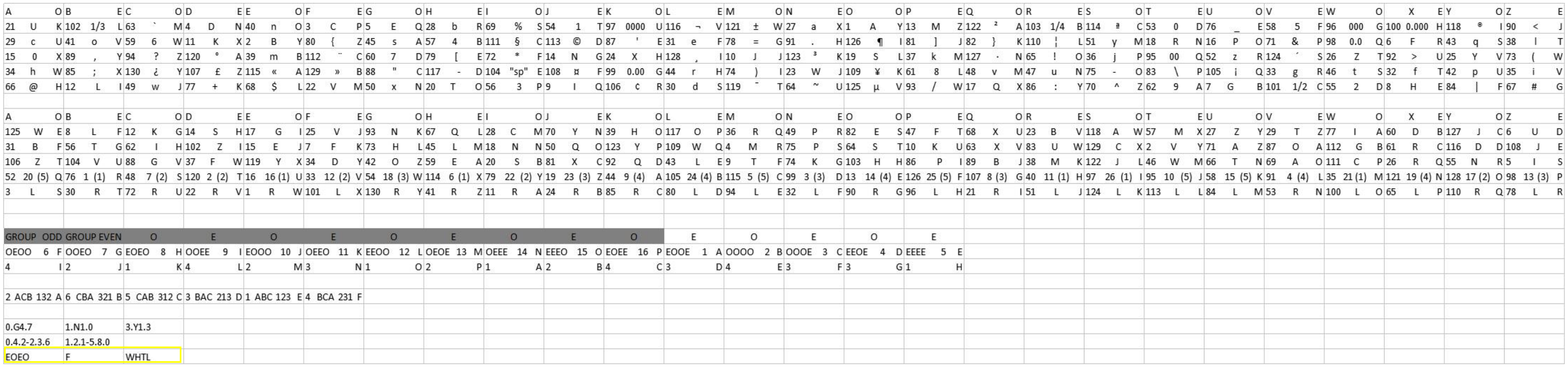
The key defines on what step it will occur (with 0 being the first before any text), what letter will be referenced, how often it will occur by frequency, and a terminus describing after how many steps it will end with zero meaning indefinite.

0.4.2-2.3.6/1.2.1-5.8.0/

Phantom shift describes on what step it will occur, on which of the five Enigma machines the shift will occur, on what counter it will occur, how many spaces forward it moves, it's frequency of occurrence, and its terminus.

This is the initial setup required for encrypting and decrypting with a given key. EOEO, F and WHTL will be our first seeds needed.

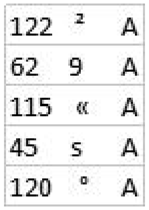
D-EOEO-V-F-WHTL-11-FI



A O	B E	C O	D E	E O	F E	G O	H E	I O	J E	K O	L E	M O	N E	O O	P E	Q O	R E	S O	T E	U O	V E	W O	X E	Y O	Z E
21 U K	102 1/3 L	63 ` M	4 D N	40 n O	3 C P	5 E Q	28 b R	69 % S	54 1 T	97 0000 U	116 ¬ V	121 ± W	27 a X	1 A Y	13 M Z	122 ² A	103 1/4 B	114 ª C	53 0 D	76 _ E	58 5 F	96 000 G	100 0.000 H	118 ® I	90 < J
29 c U	41 o V	59 6 W	11 K X	2 B Y	80 { Z	45 s A	57 4 B	111 § C	113 © D	87 ' E	31 e F	78 = G	91 . H	126 ¶ I	81] J	82 } K	110 ¦ L	51 y M	18 R N	16 P O	71 & P	98 0.0 Q	6 F R	43 q S	38 l T
15 0 X	89 , Y	94 ? Z	120 ° A	39 m B	112 ¨ C	60 7 D	79 [E	72 * F	14 N G	24 X H	128 ¸ I	10 J J	123 ³ K	19 S L	37 k M	127 · N	65 ! O	36 j P	95 00 Q	52 z R	124 ´ S	26 Z T	92 > U	25 Y V	73 (W
34 h W	85 ; X	130 ¿ Y	107 £ Z	115 « A	129 » B	88 " C	117 - D	104 "sp" E	108 ¤ F	99 0.00 G	44 r H	74) I	23 W J	109 ¥ K	61 8 L	48 v M	47 u N	75 - O	83 \ P	105 ¡ Q	33 g R	46 t S	32 f T	42 p U	35 i V
66 @ H	12 L I	49 w J	77 + K	68 $ L	22 V M	50 x N	20 T O	56 3 P	9 I Q	106 ¢ R	30 d S	119 ¯ T	64 ~ U	125 µ V	93 / W	17 Q X	86 : Y	70 ^ Z	62 9 A	7 G B	101 1/2 C	55 2 D	8 H E	84 | F	67 # G
A O	B E	C O	D E	E O	F E	G O	H E	I O	J E	K O	L E	M O	N E	O O	P E	Q O	R E	S O	T E	U O	V E	W O	X E	Y O	Z E
125 W E	8 L F	12 K G	14 S H	17 G I	25 V J	93 N K	67 Q L	28 C M	70 Y N	39 H O	117 O P	36 R Q	49 P R	82 E S	47 F T	68 X U	23 B V	118 A W	57 M X	27 Z Y	29 T Z	77 I A	60 D B	127 J C	6 U D
31 B F	56 T G	62 I H	102 Z I	15 E J	7 F K	73 H L	45 L M	18 N N	50 Q O	123 Y P	109 W Q	4 M R	75 P S	64 S T	10 K U	63 X V	83 U W	129 C X	2 V Y	71 A Z	87 O A	112 G B	61 R C	116 D D	108 J E
106 Z T	104 V U	88 G V	37 F W	119 Y X	34 D Y	42 O Z	59 E A	20 S B	81 X C	92 Q D	43 L E	9 T F	74 K G	103 H H	86 P I	89 B J	38 M K	122 J L	46 W M	66 T N	69 A O	111 C P	26 R Q	55 N R	5 I S
52 20 (5) Q	76 1 (1) R	48 7 (2) S	120 2 (2) T	16 16 (1) U	33 12 (2) V	54 18 (3) W	114 6 (1) X	79 22 (2) Y	19 23 (3) Z	44 9 (4) A	105 24 (4) B	115 5 (5) C	99 3 (3) D	13 14 (4) E	126 25 (5) F	107 8 (3) G	40 11 (1) H	97 26 (1) I	95 10 (5) J	58 15 (5) K	91 4 (4) L	35 21 (1) M	121 19 (4) N	128 17 (2) O	98 13 (3) P
3 L S	30 R T	72 R U	22 R V	1 R W	101 L X	130 R Y	41 R Z	11 R A	24 R B	85 R C	80 L D	94 L E	32 L F	90 R G	96 L H	21 R I	51 L J	124 L K	113 L L	84 L M	53 R N	100 L O	65 L P	110 R Q	78 L R
GROUP ODD	GROUP EVEN	O	E	O	E	O	E	O	E	O	E	O	E	O	E										
OEOO 6 F	OOEO 7 G	EOEO 8 H	OOEE 9 I	EOOO 10 J	OEEO 11 K	EEOO 12 L	OEOE 13 M	OEEE 14 N	EEEO 15 O	EOEE 16 P	EOOE 1 A	OOOO 2 B	OOOE 3 C	EEOE 4 D	EEEE 5 E										
4 I	2 J	1 K	4 L	2 M	3 N	1 O	2 P	1 A	2 B	4 C	3 D	4 E	3 F	3 G	1 H										
2 ACB 132 A	6 CBA 321 B	5 CAB 312 C	3 BAC 213 D	1 ABC 123 E	4 BCA 231 F																				
0.G4.7	1.N1.0	3.Y1.3																							
0.4.2-2.3.6	1.2.1-5.8.0																								
EOEO	F	WHTL																							

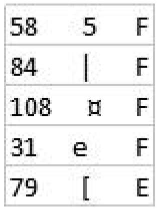
There are various rules that govern certain things. The main rule is the **first comes first and second comes second** which will reoccur throughout the process. The other rules describe forbidden Pointer field arrangements and how to deal with them. These rules prevent the duplication of pointer groups which would break the cryptographic process. It also applies when setting the Pointer field key. This rule does not apply to the Shifter or Salt field as we do not take character pointer references from them.

- No more than 3 like pointers can exist in a single column. (Since all pointers are set A-Z any columns can reference these patterns.)



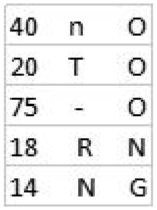
122	²	A
62	9	A
115	«	A
45	s	A
120	°	A

Not allowed



58	5	F
84	|	F
108	¤	F
31	e	F
79	[	E

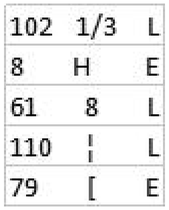
Not allowed



40	n	O
20	T	O
75	-	O
18	R	N
14	N	G

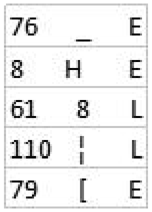
Allowed

- If 3 like pointers exist in a single column and the other 2 pointers are of themselves a like kind then the groups may not be separated.



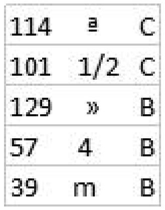
102	1/3	L
8	H	E
61	8	L
110	¦	L
79	[	E

Not allowed



76	_	E
8	H	E
61	8	L
110	¦	L
79	[	E

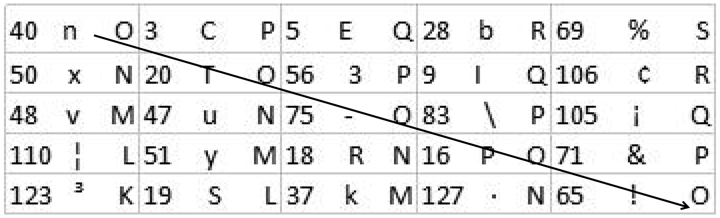
Allowed



114	ª	C
101	1/2	C
129	»	B
57	4	B
39	m	B

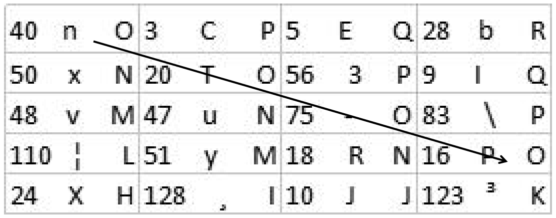
Allowed

-No more than **1 like type** of diagonal pointer arrangement may exist within a column or it's adjacent columns; 1 column must separate at minimum. There are **2 types** applicable, an up left-down right (↘) arrangement and a down left-up right (↗) arrangement and may share values.



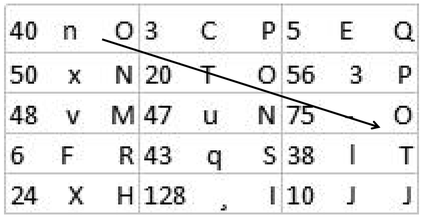
40	n	O	3	C	P	5	E	Q	28	b	R	69	%	S
50	x	N	20	T	O	56	3	P	9	I	Q	106	¢	R
48	v	M	47	u	N	75	-	O	83	\	P	105	¡	Q
110	¦	L	51	y	M	18	R	N	16	P	O	71	&	P
123	³	K	19	S	L	37	k	M	127	·	N	65	!	O

Not allowed



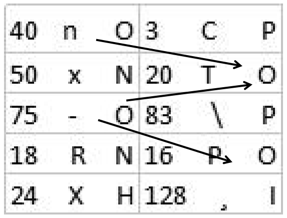
40	n	O	3	C	P	5	E	Q	28	b	R
50	x	N	20	T	O	56	3	P	9	I	Q
48	v	M	47	u	N	75	-	O	83	\	P
110	¦	L	51	y	M	18	R	N	16	P	O
24	X	H	128	¸	I	10	J	J	123	³	K

Not allowed



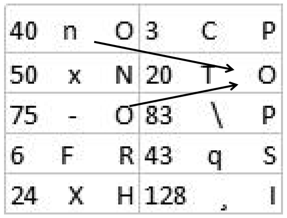
40	n	O	3	C	P	5	E	Q
50	x	N	20	T	O	56	3	P
48	v	M	47	u	N	75	-	O
6	F	R	43	q	S	38	I	T
24	X	H	128	¸	I	10	J	J

Not allowed



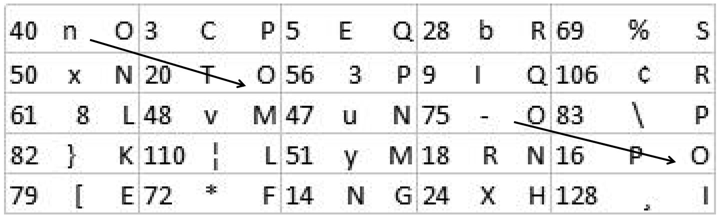
40	n	O	3	C	P
50	x	N	20	T	O
75	-	O	83	\	P
18	R	N	16	P	O
24	X	H	128	¸	I

Not allowed



40	n	O	3	C	P
50	x	N	20	T	O
75	-	O	83	\	P
6	F	R	43	q	S
24	X	H	128	¸	I

Allowed



40	n	O	3	C	P	5	E	Q	28	b	R	69	%	S
50	x	N	20	T	O	56	3	P	9	I	Q	106	¢	R
61	8	L	48	v	M	47	u	N	75	-	O	83	\	P
82	}	K	110	¦	L	51	y	M	18	R	N	16	P	O
79	[	E	72	*	F	14	N	G	24	X	H	128	¸	I

Allowed

- The Salt Field placement row always shifts one space right.

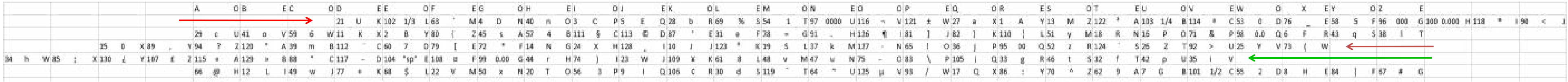
- If the paths referenced for final encryption call for the **re-use** of an Enigma machine then the we use **first comes first** rule to associate the proper machine numbers. For example if the Path is A S O A N this equates to 1, 4, 3, 1, 2 but since the 2nd A comes 2nd it holds the next value so the order goes 1, 5, 4, 2, 3. The 2nd A will still pass through machine 1 so the order for final encryption would go 1, 5, 4, 1, 3.

WBGIG -> 4, 1, 2, 3, 2 -> (2nd G comes 2nd) 5, 1, 2, 4, 3 -> (1st machine referenced) 5, 1, 2, 4, 2

HEBYY -> 3, 2, 1, 4, 4 -> 3, 2, 1, 4, 5-> 3, 2, 1, 4, 4

In simple terms we always pick the low side of the duplication. The technical drawback here is the 5th machine will never be re-used when passing a letter but spreads the possible paths out from “all letters through all machines once” to possibly between “all letters through all machines once and all letters through 2 machines once and through a 3rd machine three times”.

Shifting functions by moving rows either left or right and was achieved by copying and inserting cells to move right and deleting cells to move left. In this field row 1 shifts to the right 3 spaces, row 3 to the left 2 spaces and row 4 to the left 4 spaces.



												A		O	B		E	C		O
												29	c	U	41	o	V	59	6	W
						15	0	X	89	,	Y	94	?	Z	120	°	A	39	m	B
34	h	W	85	;	X	130	¿	Y	107	£	Z	115	«	A	129	»	B	88	"	C
												66	@	H	12	L	I	49	w	J

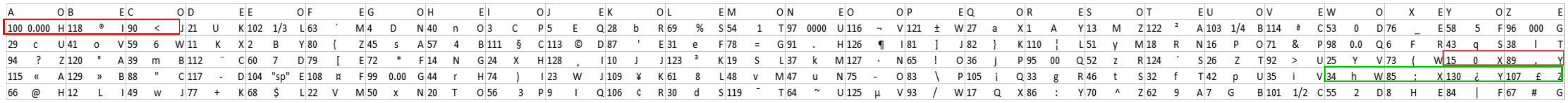
D		E	E		O	F		E	G		O	H		E	I		O	J		E
21	U	K	102	1/3	L	63	`	M	4	D	N	40	n	O	3	C	P	5	E	Q
11	K	X	2	B	Y	80	{	Z	45	s	A	57	4	B	111	§	C	113	©	D
112	¨	C	60	7	D	79	[	E	72	*	F	14	N	G	24	X	H	128	¸	I
117	-	D	104	"sp"	E	108	¤	F	99	0.00	G	44	r	H	74	)	I	23	W	J
77	+	K	68	$	L	22	V	M	50	x	N	20	T	O	56	3	P	9	I	Q

K		O	L		E	M		O	N		E	O		O	P		E	Q		O
28	b	R	69	%	S	54	1	T	97	0000	U	116	¬	V	121	±	W	27	a	X
87	'	E	31	e	F	78	=	G	91	.	H	126	¶	I	81	]	J	82	}	K
10	J	J	123	³	K	19	S	L	37	k	M	127	·	N	65	!	O	36	j	P
109	¥	K	61	8	L	48	v	M	47	u	N	75	-	O	83	\	P	105	¡	Q
106	¢	R	30	d	S	119	¯	T	64	~	U	125	µ	V	93	/	W	17	Q	X

R		E	S		O	T		E	U		O	V		E	W		O		X	E
1	A	Y	13	M	Z	122	²	A	103	1/4	B	114	ª	C	53	0	D	76	_	E
110	¦	L	51	y	M	18	R	N	16	P	O	71	&	P	98	0.0	Q	6	F	R
95	00	Q	52	z	R	124	´	S	26	Z	T	92	>	U	25	Y	V	73	(	W
33	g	R	46	t	S	32	f	T	42	p	U	35	i	V						
86	:	Y	70	^	Z	62	9	A	7	G	B	101	1/2	C	55	2	D	8	H	E

Y		O	Z		E									
58	5	F	96	000	G	100	0.000	H	118	®	I	90	<	J
43	q	S	38	l	T									
84	|	F	67	#	G									

The excess is cut and pasted into the same rows' gap to re-complete the field (this was the test method).



A		O	B		E	C		O	D		E	E		O	F		E	G		O
100	0.000	H	118	®	I	90	<	J	21	U	K	102	1/3	L	63	`	M	4	D	N
29	c	U	41	o	V	59	6	W	11	K	X	2	B	Y	80	{	Z	45	s	A
94	?	Z	120	°	A	39	m	B	112	¨	C	60	7	D	79	[	E	72	*	F
115	«	A	129	»	B	88	"	C	117	-	D	104	"sp"	E	108	¤	F	99	0.00	G
66	@	H	12	L	I	49	w	J	77	+	K	68	$	L	22	V	M	50	x	N

H		E	I		O	J		E	K		O	L		E	M		O	N		E
40	n	O	3	C	P	5	E	Q	28	b	R	69	%	S	54	1	T	97	0000	U
57	4	B	111	§	C	113	©	D	87	'	E	31	e	F	78	=	G	91	.	H
14	N	G	24	X	H	128	¸	I	10	J	J	123	³	K	19	S	L	37	k	M
44	r	H	74	)	I	23	W	J	109	¥	K	61	8	L	48	v	M	47	u	N
20	T	O	56	3	P	9	I	Q	106	¢	R	30	d	S	119	¯	T	64	~	U

O		O	P		E	Q		O	R		E	S		O	T		E
116	¬	V	121	±	W	27	a	X	1	A	Y	13	M	Z	122	²	A
126	¶	I	81	]	J	82	}	K	110	¦	L	51	y	M	18	R	N
127	·	N	65	!	O	36	j	P	95	00	Q	52	z	R	124	´	S
75	-	O	83	\	P	105	¡	Q	33	g	R	46	t	S	32	f	T
125	µ	V	93	/	W	17	Q	X	86	:	Y	70	^	Z	62	9	A

U		O	V		E	W		O		X	E	Y		O	Z		E
103	1/4	B	114	ª	C	53	0	D	76	_	E	58	5	F	96	000	G
16	P	O	71	&	P	98	0.0	Q	6	F	R	43	q	S	38	l	T
26	Z	T	92	>	U	25	Y	V	73	(	W	15	0	X	89	,	Y
42	p	U	35	i	V	34	h	W	85	;	X	130	¿	Y	107	£	Z
7	G	B	101	1/2	C	55	2	D	8	H	E	84	|	F	67	#	G

At the end of the shifting, which occurs as the last step of each characters encryption/decryption, the Pointer field is assessed for rule compliance.

The **forcing rule** proceeds as follows.

- the 2nd row that was shifted moves one space in the same direction of its prior shift and the field is again assessed for rule compliance
- repeat for the 3rd row
- repeat for the 4th row
- return to 1st step (feasibly at most only 4 rules enforcement steps should be required)

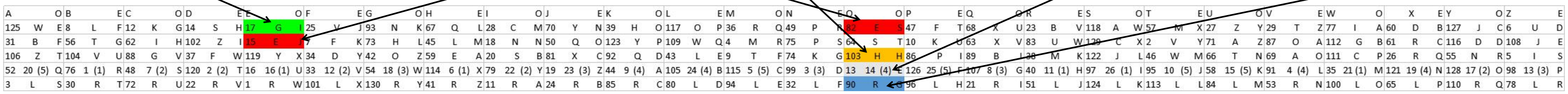
START 1

To encrypt a message we begin by assessing a Polyphasic salt seed. **If yes** we assess the **first one first**.

0.G4.7/3.Y1.3/1.N1.0/

On step 0 (zero), pass the conversion for G, every 4th step, terminating after the 7th occourance.

We correlate the Polyphasic salt seed from the shifter field its 1) conversion, 2) specific column, 3) the "spaces" number for its even or odd and beginning row 4) and Direction.

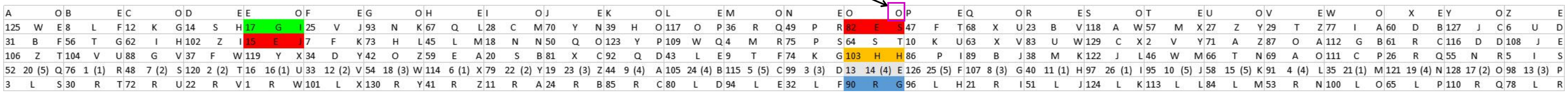


A		O	B		E	C		O	D		E	E		O	F		E	G		O	H		E	I		O	J		E	K		O	L		E	M		O
125	W	E	8	L	F	12	K	G	14	S	H	17	G	I	25	V	J	93	N	K	67	Q	L	28	C	M	70	Y	N	39	H	O	117	O	P	36	R	Q
31	B	F	56	T	G	62	I	H	102	Z	I	15	E	J	7	F	K	73	H	L	45	L	M	18	N	N	50	Q	O	123	Y	P	109	W	Q	4	M	R
106	Z	T	104	V	U	88	G	V	37	F	W	119	Y	X	34	D	Y	42	O	Z	59	E	A	20	S	B	81	X	C	92	Q	D	43	L	E	9	T	F
52	20 (5)	Q	76	1 (1)	R	48	7 (2)	S	120	2 (2)	T	16	16 (1)	U	33	12 (2)	V	54	18 (3)	W	114	6 (1)	X	79	22 (2)	Y	19	23 (3)	Z	44	9 (4)	A	105	24 (4)	B	115	5 (5)	C
3	L	S	30	R	T	72	R	U	22	R	V	1	R	W	101	L	X	130	R	Y	41	R	Z	11	R	A	24	R	B	85	R	C	80	L	D	94	L	E

N		E	O		O	P		E	Q		O	R		E	S		O	T		E	U		O	V		E	W		O		X	E	Y		O	Z		E
49	P	R	82	E	S	47	F	T	68	X	U	23	B	V	118	A	W	57	M	X	27	Z	Y	29	T	Z	77	I	A	60	D	B	127	J	C	6	U	D
75	P	S	64	S	T	10	K	U	63	X	V	83	U	W	129	C	X	2	V	Y	71	A	Z	87	O	A	112	G	B	61	R	C	116	D	D	108	J	E
74	K	G	103	H	H	86	P	I	89	B	J	38	M	K	122	J	L	46	W	M	66	T	N	69	A	O	111	C	P	26	R	Q	55	N	R	5	I	S
99	3 (3)	D	13	14 (4)	E	126	25 (5)	F	107	8 (3)	G	40	11 (1)	H	97	26 (1)	I	95	10 (5)	J	58	15 (5)	K	91	4 (4)	L	35	21 (1)	M	121	19 (4)	N	128	17 (2)	O	98	13 (3)	P
32	L	F	90	R	G	96	L	H	21	R	I	51	L	J	124	L	K	113	L	L	84	L	M	53	R	N	100	L	O	65	L	P	110	R	Q	78	L	R

If its conversion is Even we assess from the **Shifter field**. If its conversion is **Odd** we assess from the P**ointer field.** We assess this value from the Hard row.

ODD



A		O	B		E	C		O	D		E	E		O	F		E	G		O	H		E	I		O	J		E	K		O	L		E	M		O
125	W	E	8	L	F	12	K	G	14	S	H	17	G	I	25	V	J	93	N	K	67	Q	L	28	C	M	70	Y	N	39	H	O	117	O	P	36	R	Q
31	B	F	56	T	G	62	I	H	102	Z	I	15	E	J	7	F	K	73	H	L	45	L	M	18	N	N	50	Q	O	123	Y	P	109	W	Q	4	M	R
106	Z	T	104	V	U	88	G	V	37	F	W	119	Y	X	34	D	Y	42	O	Z	59	E	A	20	S	B	81	X	C	92	Q	D	43	L	E	9	T	F
52	20 (5)	Q	76	1 (1)	R	48	7 (2)	S	120	2 (2)	T	16	16 (1)	U	33	12 (2)	V	54	18 (3)	W	114	6 (1)	X	79	22 (2)	Y	19	23 (3)	Z	44	9 (4)	A	105	24 (4)	B	115	5 (5)	C
3	L	S	30	R	T	72	R	U	22	R	V	1	R	W	101	L	X	130	R	Y	41	R	Z	11	R	A	24	R	B	85	R	C	80	L	D	94	L	E

N		E	O		O	P		E	Q		O	R		E	S		O	T		E	U		O	V		E	W		O		X	E	Y		O	Z		E
49	P	R	82	E	S	47	F	T	68	X	U	23	B	V	118	A	W	57	M	X	27	Z	Y	29	T	Z	77	I	A	60	D	B	127	J	C	6	U	D
75	P	S	64	S	T	10	K	U	63	X	V	83	U	W	129	C	X	2	V	Y	71	A	Z	87	O	A	112	G	B	61	R	C	116	D	D	108	J	E
74	K	G	103	H	H	86	P	I	89	B	J	38	M	K	122	J	L	46	W	M	66	T	N	69	A	O	111	C	P	26	R	Q	55	N	R	5	I	S
99	3 (3)	D	13	14 (4)	E	126	25 (5)	F	107	8 (3)	G	40	11 (1)	H	97	26 (1)	I	95	10 (5)	J	58	15 (5)	K	91	4 (4)	L	35	21 (1)	M	121	19 (4)	N	128	17 (2)	O	98	13 (3)	P
32	L	F	90	R	G	96	L	H	21	R	I	51	L	J	124	L	K	113	L	L	84	L	M	53	R	N	100	L	O	65	L	P	110	R	Q	78	L	R

The letter for the 2nd conversion row points to the specific column from which the path will be referenced.

If the specific value of the spaces row is **Even**, the **letter pointers** on the field will be referenced for the height.

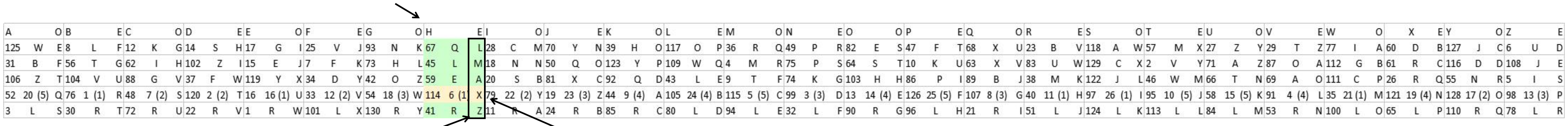
If **Odd**, the **number**s will be referenced for the height.

The spaces row also determines from which row we will begin referencing the values shown in parenthesis.

The direction of the reference taken from the direction row is correlated to **left=down and right=up.**

In this case the hard row is Odd, the conversion is E, the column is H, the spaces is Even, the row is (4), the direction is UP

Odd = Shifter field


column H

A		O	B		E	C		O	D		E	E		O
125	W	E	8	L	F	12	K	G	14	S	H	17	G	I
31	B	F	56	T	G	62	I	H	102	Z	I	15	E	J
106	Z	T	104	V	U	88	G	V	37	F	W	119	Y	X
52	20 (5)	Q	76	1 (1)	R	48	7 (2)	S	120	2 (2)	T	16	16 (1)	U
3	L	S	30	R	T	72	R	U	22	R	V	1	R	W

F		E	G		O	H		E	I		O	J		E
25	V	J	93	N	K	67	Q	L	28	C	M	70	Y	N
7	F	K	73	H	L	45	L	M	18	N	N	50	Q	O
34	D	Y	42	O	Z	59	E	A	20	S	B	81	X	C
33	12 (2)	V	54	18 (3)	W	114	6 (1)	X	79	22 (2)	Y	19	23 (3)	Z
101	L	X	130	R	Y	41	R	Z	11	R	A	24	R	B

K		O	L		E	M		O	N		E	O		O
39	H	O	117	O	P	36	R	Q	49	P	R	82	E	S
123	Y	P	109	W	Q	4	M	R	75	P	S	64	S	T
92	Q	D	43	L	E	9	T	F	74	K	G	103	H	H
44	9 (4)	A	105	24 (4)	B	115	5 (5)	C	99	3 (3)	D	13	14 (4)	E
85	R	C	80	L	D	94	L	E	32	L	F	90	R	G

P		E	Q		O	R		E	S		O	T		E
47	F	T	68	X	U	23	B	V	118	A	W	57	M	X
10	K	U	63	X	V	83	U	W	129	C	X	2	V	Y
86	P	I	89	B	J	38	M	K	122	J	L	46	W	M
126	25 (5)	F	107	8 (3)	G	40	11 (1)	H	97	26 (1)	I	95	10 (5)	J
96	L	H	21	R	I	51	L	J	124	L	K	113	L	L

U		O	V		E	W		O		X	E	Y		O	Z		E
27	Z	Y	29	T	Z	77	I	A	60	D	B	127	J	C	6	U	D
71	A	Z	87	O	A	112	G	B	61	R	C	116	D	D	108	J	E
66	T	N	69	A	O	111	C	P	26	R	Q	55	N	R	5	I	S
58	15 (5)	K	91	4 (4)	L	35	21 (1)	M	121	19 (4)	N	128	17 (2)	O	98	13 (3)	P
84	L	M	53	R	N	100	L	O	65	L	P	110	R	Q	78	L	R

Path reference letters

Starting row 4, move up

We reference the path for the conversion of our salt value by its height and pass it through the five Enigma machines.

Path -> X A M L Z -> 4, 1, 3, 2, 5 -> Pass E through machines in order 4, 1, 3, 2, 5 -> Output-> H

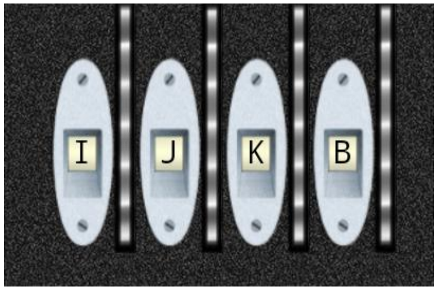
If no, we continue.

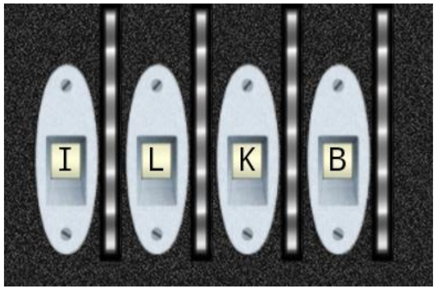
Next, we assess the first Phantom shift. **If yes** we assess the the value seeded in the key and execute.

0.4.2-2.3.6/1.2.1-5.8.0/

On step 0 (zero),on machine 4, on counter 2 move forward 2 letters after every 3rd step, terminating after the 6th occurance.

J -> K -> L



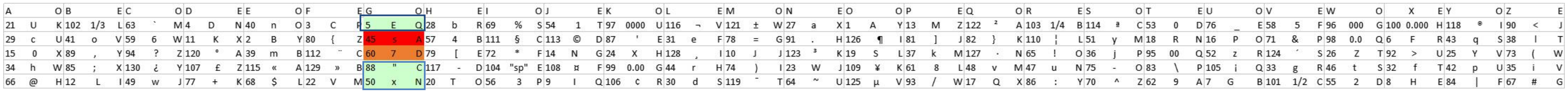


If no, we continue.

We then repeat by assessing for 2nd , 3rd etc. Polyphasic salt and Phantom shifting parameters. **If yes,** we repeat the process for the steps above. The parameters follow the same linear causality, if the same character appears on the same step the **first goes first.**

If no, we continue.

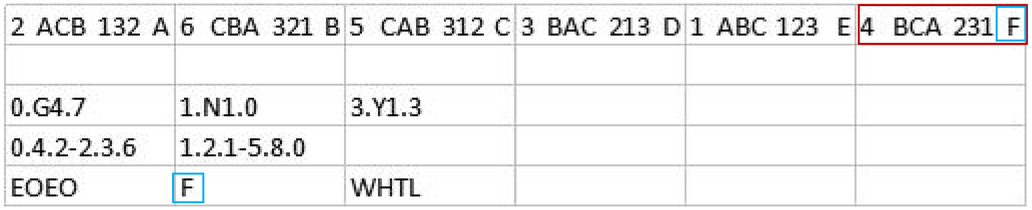
We locate the desired char (we'll select "7") on the pointer field and assess it's associated pointer set which are the **3 letters immediately below** the desired cell with the **fourth letter constituting the salt**. (If the reference goes off of the field it returns to the opposite side as though it were on a cylinder.)



A		O	B		E	C		O	D		E	E		O	F		E	G		O	H		E	I		O	J		E	K		O	L		E	M		O	N		E	O		O	P		E	Q		O	R		E	S		O	T		E	U		O	V		E	W		O		X	E	Y		O	Z		E
21	U	K	102	1/3	L	63	`	M	4	D	N	40	n	O	3	C	P	5	E	Q	28	b	R	69	%	S	54	1	T	97	0000	U	116	¬	V	121	±	W	27	a	X	1	A	Y	13	M	Z	122	²	A	103	1/4	B	114	ª	C	53	0	D	76	_	E	58	5	F	96	000	G	100	0.000	H	118	®	I	90	<	J
29	c	U	41	o	V	59	6	W	11	K	X	2	B	Y	80	{	Z	45	s	A	57	4	B	111	§	C	113	©	D	87	'	E	31	e	F	78	=	G	91	.	H	126	¶	I	81	]	J	82	}	K	110	¦	L	51	y	M	18	R	N	16	P	O	71	&	P	98	0.0	Q	6	F	R	43	q	S	38	l	T
15	0	X	89	,	Y	94	?	Z	120	°	A	39	m	B	112	¨	C	60	7	D	79	[	E	72	*	F	14	N	G	24	X	H	128	¸	I	10	J	J	123	³	K	19	S	L	37	k	M	127	·	N	65	!	O	36	j	P	95	00	Q	52	z	R	124	´	S	26	Z	T	92	>	U	25	Y	V	73	(	W
34	h	W	85	;	X	130	¿	Y	107	£	Z	115	«	A	129	»	B	88	"	C	117	-	D	104	"sp"	E	108	¤	F	99	0.00	G	44	r	H	74	)	I	23	W	J	109	¥	K	61	8	L	48	v	M	47	u	N	75	-	O	83	\	P	105	¡	Q	33	g	R	46	t	S	32	f	T	42	p	U	35	i	V
66	@	H	12	L	I	49	w	J	77	+	K	68	$	L	22	V	M	50	x	N	20	T	O	56	3	P	9	I	Q	106	¢	R	30	d	S	119	¯	T	64	~	U	125	µ	V	93	/	W	17	Q	X	86	:	Y	70	^	Z	62	9	A	7	G	B	101	1/2	C	55	2	D	8	H	E	84	|	F	67	#	G

The initial pointer group for "7" is C N Q and Phasic salt is A.

For CNQ (ABC) we assess the Slide seed for the shift value and shift the pointer set.

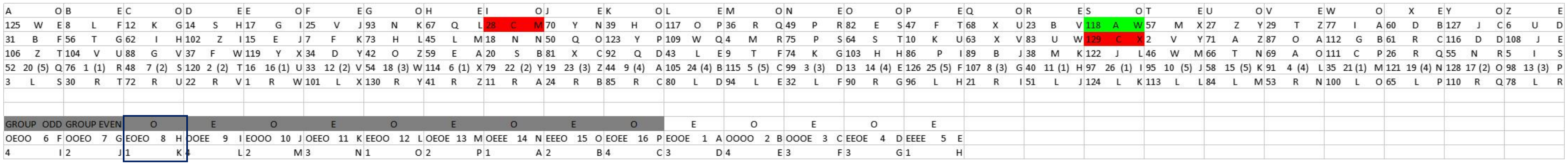


2 ACB 132 A	6 CBA 321 B	5 CAB 312 C	3 BAC 213 D	1 ABC 123 E	4 BCA 231 F
0.G4.7	1.N1.0	3.Y1.3			
0.4.2-2.3.6	1.2.1-5.8.0				
EOEO	F	WHTL			

The Slide seed is F which correlates to BCA 231 which indicates the first letter is moved to the last position giving NCQ. (QNC = ABC -> NCQ = BCA)

The new pointer set is referenced for a new seed value for the Slider field by assessing the numeric equivalency of its letters. (For NQC we get 231 again)

We then reference Phasic salt (D) to its conversion on the salt conversion row and assess the EO seed for possible salt placement.



A		O	B		E	C		O	D		E	E		O	F		E	G		O	H		E	I		O	J		E	K		O	L		E	M		O	N		E	O		O	P		E	Q		O	R		E	S		O	T		E	U		O	V		E	W		O		X	E	Y		O	Z		E
125	W	E	8	L	F	12	K	G	14	S	H	17	G	I	25	V	J	93	N	K	67	Q	L	28	C	M	70	Y	N	39	H	O	117	O	P	36	R	Q	49	P	R	82	E	S	47	F	T	68	X	U	23	B	V	118	A	W	57	M	X	27	Z	Y	29	T	Z	77	I	A	60	D	B	127	J	C	6	U	D
31	B	F	56	T	G	62	I	H	102	Z	I	15	E	J	7	F	K	73	H	L	45	L	M	18	N	N	50	Q	O	123	Y	P	109	W	Q	4	M	R	75	P	S	64	S	T	10	K	U	63	X	V	83	U	W	129	C	X	2	V	Y	71	A	Z	87	O	A	112	G	B	61	R	C	116	D	D	108	J	E
106	Z	T	104	V	U	88	G	V	37	F	W	119	Y	X	34	D	Y	42	O	Z	59	E	A	20	S	B	81	X	C	92	Q	D	43	L	E	9	T	F	74	K	G	103	H	H	86	P	I	89	B	J	38	M	K	122	J	L	46	W	M	66	T	N	69	A	O	111	C	P	26	R	Q	55	N	R	5	I	S
52	20 (5)	Q	76	1 (1)	R	48	7 (2)	S	120	2 (2)	T	16	16 (1)	U	33	12 (2)	V	54	18 (3)	W	114	6 (1)	X	79	22 (2)	Y	19	23 (3)	Z	44	9 (4)	A	105	24 (4)	B	115	5 (5)	C	99	3 (3)	D	13	14 (4)	E	126	25 (5)	F	107	8 (3)	G	40	11 (1)	H	97	26 (1)	I	95	10 (5)	J	58	15 (5)	K	91	4 (4)	L	35	21 (1)	M	121	19 (4)	N	128	17 (2)	O	98	13 (3)	P
3	L	S	30	R	T	72	R	U	22	R	V	1	R	W	101	L	X	130	R	Y	41	R	Z	11	R	A	24	R	B	85	R	C	80	L	D	94	L	E	32	L	F	90	R	G	96	L	H	21	R	I	51	L	J	124	L	K	113	L	L	84	L	M	53	R	N	100	L	O	65	L	P	110	R	Q	78	L	R
GROUP	ODD		GROUP EVEN			O			E			O			E			O			E			O			E			O			E			O			E			O			E																																
OEOO	6	F	OOEO	7	G	EOEO	8	H	OOEE	9	I	EOOO	10	J	OEEO	11	K	EEOO	12	L	OEOE	13	M	OEEE	14	N	EEEO	15	O	EOEE	16	P	EOOE	1	A	OOOO	2	B	OOOE	3	C	EEOE	4	D	EEEE	5	E																														
4		I	2		J	1		K	4		L	2		M	3		N	1		O	2		P	1		A	2		B	4		C	3		D	4		E	3		F	3		G	1		H																														

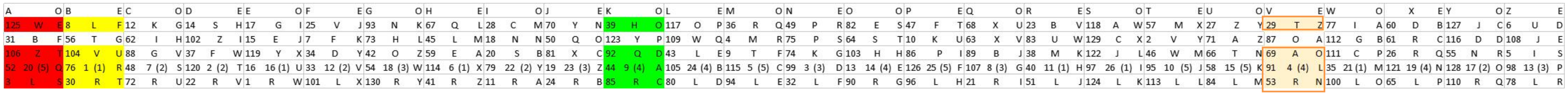
If yes, we place the conversion letter into referenced location. A converts to C, EOEO is active and the position is 1. We place C into NCQ into position 1 giving CNCQ.

N C Q
↑ ↑ ↑ ↑
Position 1 2 3 4

We then take a reference of the new pointer set for a new EO seed by assessing the numeric equivalency of its letters to Even or Odd. For the EO seed CNCQ we get OEOO.

If no, we impose the salt (D) into it's would be location as above and take a reference for the new EO seed. We then remove salt (D). This allows a variance of the output length for each group.

We then reference the Height seed against the correlation row to find the enigma paths for the text input. This is done in the same manner as the Polyphasic salt. We use the specific letters as they would have been converted on the previous round. We also take a new Height seed reference from the conversion row. The new Height seed is BYTO.



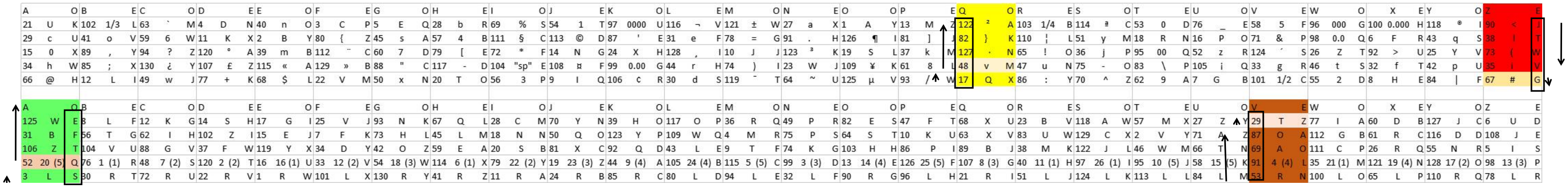
A		O	B		E	C		O	D		E	E		O	F		E	G		O	H		E	I		O	J		E	K		O	L		E	M		O	N		E	O		O	P		E	Q		O	R		E	S		O	T		E	U		O	V		E	W		O		X	E	Y		O	Z		E
125	W	E	8	L	F	12	K	G	14	S	H	17	G	I	25	V	J	93	N	K	67	Q	L	28	C	M	70	Y	N	39	H	O	117	O	P	36	R	Q	49	P	R	82	E	S	47	F	T	68	X	U	23	B	V	118	A	W	57	M	X	27	Z	Y	29	T	Z	77	I	A	60	D	B	127	J	C	6	U	D
31	B	F	56	T	G	62	I	H	102	Z	I	15	E	J	7	F	K	73	H	L	45	L	M	18	N	N	50	Q	O	123	Y	P	109	W	Q	4	M	R	75	P	S	64	S	T	10	K	U	63	X	V	83	U	W	129	C	X	2	V	Y	71	A	Z	87	O	A	112	G	B	61	R	C	116	D	D	108	J	E
106	Z	T	104	V	U	88	G	V	37	F	W	119	Y	X	34	D	Y	42	O	Z	59	E	A	20	S	B	81	X	C	92	Q	D	43	L	E	9	T	F	74	K	G	103	H	H	86	P	I	89	B	J	38	M	K	122	J	L	46	W	M	66	T	N	69	A	O	111	C	P	26	R	Q	55	N	R	5	I	S
52	20 (5)	Q	76	1 (1)	R	48	7 (2)	S	120	2 (2)	T	16	16 (1)	U	33	12 (2)	V	54	18 (3)	W	114	6 (1)	X	79	22 (2)	Y	19	23 (3)	Z	44	9 (4)	A	105	24 (4)	B	115	5 (5)	C	99	3 (3)	D	13	14 (4)	E	126	25 (5)	F	107	8 (3)	G	40	11 (1)	H	97	26 (1)	I	95	10 (5)	J	58	15 (5)	K	91	4 (4)	L	35	21 (1)	M	121	19 (4)	N	128	17 (2)	O	98	13 (3)	P
3	L	S	30	R	T	72	R	U	22	R	V	1	R	W	101	L	X	130	R	Y	41	R	Z	11	R	A	24	R	B	85	R	C	80	L	D	94	L	E	32	L	F	90	R	G	96	L	H	21	R	I	51	L	J	124	L	K	113	L	L	84	L	M	53	R	N	100	L	O	65	L	P	110	R	Q	78	L	R

1) W -> Odd(pointer field), column Z, Even(letters) row 5, down -> G J T W V -> 1, 2, 3, 5, 4

2) H-> Odd(pointer field), column Q, Odd(numbers) row 4, up -> 48, 127, 82, 122, 17 -> 2, 5, 3, 4, 1

3) T-> Even(shifter field), column A, Even(letters) row 4, up -> Q, T, F, E, S -> 3, 5, 2, 1, 4

4) L-> Even(shifter field), column V, Odd(numbers) row 1, up -> 29, 53, 91, 89, 87 -> 1, 2, 5, 4, 3



A		O	B		E	C		O	D		E	E		O	F		E	G		O	H		E	I		O	J		E	K		O	L		E	M		O	N		E	O		O	P		E	Q		O	R		E	S		O	T		E	U		O	V		E	W		O		X	E	Y		O	Z		E
21	U	K	102	1/3	L	63	`	M	4	D	N	40	n	O	3	C	P	5	E	Q	28	b	R	69	%	S	54	1	T	97	0000	U	116	¬	V	121	±	W	27	a	X	1	A	Y	13	M	Z	122	²	A	103	1/4	B	114	ª	C	53	0	D	76	_	E	58	5	F	96	000	G	100	0.000	H	118	®	I	90	<	J
29	c	U	41	o	V	59	6	W	11	K	X	2	B	Y	80	{	Z	45	s	A	57	4	B	111	§	C	113	©	D	87	'	E	31	e	F	78	=	G	91	.	H	126	¶	I	81	]	J	82	}	K	110	¦	L	51	y	M	18	R	N	16	P	O	71	&	P	98	0.0	Q	6	F	R	43	q	S	38	l	T
15	0	X	89	,	Y	94	?	Z	120	°	A	39	m	B	112	¨	C	60	7	D	79	[	E	72	*	F	14	N	G	24	X	H	128	¸	I	10	J	J	123	³	K	19	S	L	37	k	M	127	·	N	65	!	O	36	j	P	95	00	Q	52	z	R	124	´	S	26	Z	T	92	>	U	25	Y	V	73	(	W
34	h	W	85	;	X	130	¿	Y	107	£	Z	115	«	A	129	»	B	88	"	C	117	-	D	104	"sp"	E	108	¤	F	99	0.00	G	44	r	H	74	)	I	23	W	J	109	¥	K	61	8	L	48	v	M	47	u	N	75	-	O	83	\	P	105	¡	Q	33	g	R	46	t	S	32	f	T	42	p	U	35	i	V
66	@	H	12	L	I	49	w	J	77	+	K	68	$	L	22	V	M	50	x	N	20	T	O	56	3	P	9	I	Q	106	¢	R	30	d	S	119	¯	T	64	~	U	125	µ	V	93	/	W	17	Q	X	86	:	Y	70	^	Z	62	9	A	7	G	B	101	1/2	C	55	2	D	8	H	E	84	|	F	67	#	G

A		O	B		E	C		O	D		E	E		O	F		E	G		O	H		E	I		O	J		E	K		O	L		E	M		O	N		E	O		O	P		E	Q		O	R		E	S		O	T		E	U		O	V		E	W		O		X	E	Y		O	Z		E
125	W	E	8	L	F	12	K	G	14	S	H	17	G	I	25	V	J	93	N	K	67	Q	L	28	C	M	70	Y	N	39	H	O	117	O	P	36	R	Q	49	P	R	82	E	S	47	F	T	68	X	U	23	B	V	118	A	W	57	M	X	27	Z	Y	29	T	Z	77	I	A	60	D	B	127	J	C	6	U	D
31	B	F	56	T	G	62	I	H	102	Z	I	15	E	J	7	F	K	73	H	L	45	L	M	18	N	N	50	Q	O	123	Y	P	109	W	Q	4	M	R	75	P	S	64	S	T	10	K	U	63	X	V	83	U	W	129	C	X	2	V	Y	71	A	Z	87	O	A	112	G	B	61	R	C	116	D	D	108	J	E
106	Z	T	104	V	U	88	G	V	37	F	W	119	Y	X	34	D	Y	42	O	Z	59	E	A	20	S	B	81	X	C	92	Q	D	43	L	E	9	T	F	74	K	G	103	H	H	86	P	I	89	B	J	38	M	K	122	J	L	46	W	M	66	T	N	69	A	O	111	C	P	26	R	Q	55	N	R	5	I	S
52	20 (5)	Q	76	1 (1)	R	48	7 (2)	S	120	2 (2)	T	16	16 (1)	U	33	12 (2)	V	54	18 (3)	W	114	6 (1)	X	79	22 (2)	Y	19	23 (3)	Z	44	9 (4)	A	105	24 (4)	B	115	5 (5)	C	99	3 (3)	D	13	14 (4)	E	126	25 (5)	F	107	8 (3)	G	40	11 (1)	H	97	26 (1)	I	95	10 (5)	J	58	15 (5)	K	91	4 (4)	L	35	21 (1)	M	121	19 (4)	N	128	17 (2)	O	98	13 (3)	P
3	L	S	30	R	T	72	R	U	22	R	V	1	R	W	101	L	X	130	R	Y	41	R	Z	11	R	A	24	R	B	85	R	C	80	L	D	94	L	E	32	L	F	90	R	G	96	L	H	21	R	I	51	L	J	124	L	K	113	L	L	84	L	M	53	R	N	100	L	O	65	L	P	110	R	Q	78	L	R

We then pass the pointer group through these paths one letter at a time to produce the encrypted output text.

C -> 1, 2, 3, 5, 4 -> Output D

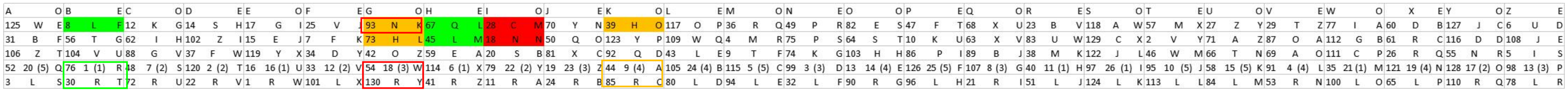
N -> 2, 5, 3, 4, 1-> Output R

C -> 3, 5, 2, 1, 4-> Output Z

Q -> 1, 2, 5, 4, 3-> Output C

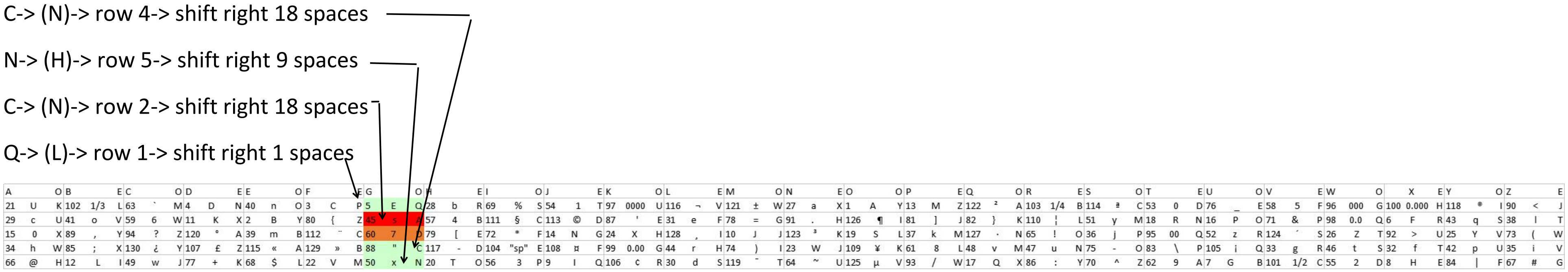
The current output string is H D R Z C.

Shifting functions the same for both encryption and decryption. We assess the shift values for the Pointer field by referencing the pointers first conversion values and apply them to the row from which they were derived. Most commonly 4 separate values are derived but possibly minimum 1, in which case 4 rows would shift the same direction and spaces against 1 row and the Hard row.



A		O	B		E	C		O	D		E	E		O	F		E	G		O	H		E	I		O	J		E	K		O	L		E	M		O
125	W	E	8	L	F	12	K	G	14	S	H	17	G	I	25	V	J	93	N	K	67	Q	L	28	C	M	70	Y	N	39	H	O	117	O	P	36	R	Q
31	B	F	56	T	G	62	I	H	102	Z	I	15	E	J	7	F	K	73	H	L	45	L	M	18	N	N	50	Q	O	123	Y	P	109	W	Q	4	M	R
106	Z	T	104	V	U	88	G	V	37	F	W	119	Y	X	34	D	Y	42	O	Z	59	E	A	20	S	B	81	X	C	92	Q	D	43	L	E	9	T	F
52	20 (5)	Q	76	1 (1)	R	48	7 (2)	S	120	2 (2)	T	16	16 (1)	U	33	12 (2)	V	54	18 (3)	W	114	6 (1)	X	79	22 (2)	Y	19	23 (3)	Z	44	9 (4)	A	105	24 (4)	B	115	5 (5)	C
3	L	S	30	R	T	72	R	U	22	R	V	1	R	W	101	L	X	130	R	Y	41	R	Z	11	R	A	24	R	B	85	R	C	80	L	D	94	L	E

N		E	O		O	P		E	Q		O	R		E	S		O	T		E	U		O	V		E	W		O		X	E	Y		O	Z		E
49	P	R	82	E	S	47	F	T	68	X	U	23	B	V	118	A	W	57	M	X	27	Z	Y	29	T	Z	77	I	A	60	D	B	127	J	C	6	U	D
75	P	S	64	S	T	10	K	U	63	X	V	83	U	W	129	C	X	2	V	Y	71	A	Z	87	O	A	112	G	B	61	R	C	116	D	D	108	J	E
74	K	G	103	H	H	86	P	I	89	B	J	38	M	K	122	J	L	46	W	M	66	T	N	69	A	O	111	C	P	26	R	Q	55	N	R	5	I	S
99	3 (3)	D	13	14 (4)	E	126	25 (5)	F	107	8 (3)	G	40	11 (1)	H	97	26 (1)	I	95	10 (5)	J	58	15 (5)	K	91	4 (4)	L	35	21 (1)	M	121	19 (4)	N	128	17 (2)	O	98	13 (3)	P
32	L	F	90	R	G	96	L	H	21	R	I	51	L	J	124	L	K	113	L	L	84	L	M	53	R	N	100	L	O	65	L	P	110	R	Q	78	L	R



C-> (N)-> row 4-> shift right 18 spaces

N-> (H)-> row 5-> shift right 9 spaces

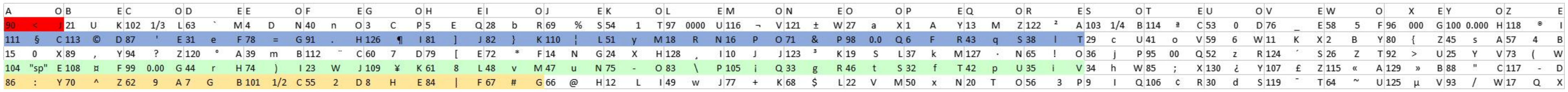
C-> (N)-> row 2-> shift right 18 spaces

Q-> (L)-> row 1-> shift right 1 spaces

A		O	B		E	C		O	D		E	E		O	F		E	G		O	H		E	I		O	J		E	K		O	L		E	M		O
21	U	K	102	1/3	L	63	`	M	4	D	N	40	n	O	3	C	P	5	E	Q	28	b	R	69	%	S	54	1	T	97	0000	U	116	¬	V	121	±	W
29	c	U	41	o	V	59	6	W	11	K	X	2	B	Y	80	{	Z	45	s	A	57	4	B	111	§	C	113	©	D	87	'	E	31	e	F	78	=	G
15	0	X	89	,	Y	94	?	Z	120	°	A	39	m	B	112	¨	C	60	7	D	79	[	E	72	*	F	14	N	G	24	X	H	128	¸	I	10	J	J
34	h	W	85	;	X	130	¿	Y	107	£	Z	115	«	A	129	»	B	88	"	C	117	-	D	104	"sp"	E	108	¤	F	99	0.00	G	44	r	H	74	)	I
66	@	H	12	L	I	49	w	J	77	+	K	68	$	L	22	V	M	50	x	N	20	T	O	56	3	P	9	I	Q	106	¢	R	30	d	S	119	¯	T

N		E	O		O	P		E	Q		O	R		E	S		O	T		E	U		O	V		E	W		O		X	E	Y		O	Z		E
27	a	X	1	A	Y	13	M	Z	122	²	A	103	1/4	B	114	ª	C	53	0	D	76	_	E	58	5	F	96	000	G	100	0.000	H	118	®	I	90	<	J
91	.	H	126	¶	I	81	]	J	82	}	K	110	¦	L	51	y	M	18	R	N	16	P	O	71	&	P	98	0.0	Q	6	F	R	43	q	S	38	l	T
123	³	K	19	S	L	37	k	M	127	·	N	65	!	O	36	j	P	95	00	Q	52	z	R	124	´	S	26	Z	T	92	>	U	25	Y	V	73	(	W
23	W	J	109	¥	K	61	8	L	48	v	M	47	u	N	75	-	O	83	\	P	105	¡	Q	33	g	R	46	t	S	32	f	T	42	p	U	35	i	V
64	~	U	125	µ	V	93	/	W	17	Q	X	86	:	Y	70	^	Z	62	9	A	7	G	B	101	1/2	C	55	2	D	8	H	E	84	|	F	67	#	G

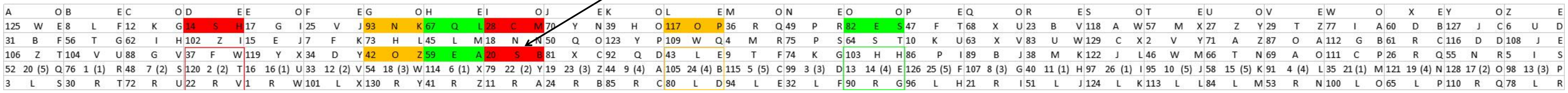
The Pointer field is shifted.



A		O	B		E	C		O	D		E	E		O	F		E	G		O	H		E	I		O	J		E	K		O	L		E	M		O
90	<	J	21	U	K	102	1/3	L	63	`	M	4	D	N	40	n	O	3	C	P	5	E	Q	28	b	R	69	%	S	54	1	T	97	0000	U	116	¬	V
111	§	C	113	©	D	87	'	E	31	e	F	78	=	G	91	.	H	126	¶	I	81	]	J	82	}	K	110	¦	L	51	y	M	18	R	N	16	P	O
15	0	X	89	,	Y	94	?	Z	120	°	A	39	m	B	112	¨	C	60	7	D	79	[	E	72	*	F	14	N	G	24	X	H	128	¸	I	10	J	J
104	"sp"	E	108	¤	F	99	0.00	G	44	r	H	74	)	I	23	W	J	109	¥	K	61	8	L	48	v	M	47	u	N	75	-	O	83	\	P	105	¡	Q
86	:	Y	70	^	Z	62	9	A	7	G	B	101	1/2	C	55	2	D	8	H	E	84	|	F	67	#	G	66	@	H	12	L	I	49	w	J	77	+	K

N		E	O		O	P		E	Q		O	R		E	S		O	T		E	U		O	V		E	W		O		X	E	Y		O	Z		E
121	±	W	27	a	X	1	A	Y	13	M	Z	122	²	A	103	1/4	B	114	ª	C	53	0	D	76	_	E	58	5	F	96	000	G	100	0.000	H	118	®	I
71	&	P	98	0.0	Q	6	F	R	43	q	S	38	l	T	29	c	U	41	o	V	59	6	W	11	K	X	2	B	Y	80	{	Z	45	s	A	57	4	B
123	³	K	19	S	L	37	k	M	127	·	N	65	!	O	36	j	P	95	00	Q	52	z	R	124	´	S	26	Z	T	92	>	U	25	Y	V	73	(	W
33	g	R	46	t	S	32	f	T	42	p	U	35	i	V	34	h	W	85	;	X	130	¿	Y	107	£	Z	115	«	A	129	»	B	88	"	C	117	-	D
68	$	L	22	V	M	50	x	N	20	T	O	56	3	P	9	I	Q	106	¢	R	30	d	S	119	¯	T	64	~	U	125	µ	V	93	/	W	17	Q	X

We assess the shift values for the Shifter field by referencing the 2nd conversions and executing in the same manner.



A		O	B		E	C		O	D		E	E		O	F		E	G		O	H		E	I		O	J		E	K		O	L		E	M		O
125	W	E	8	L	F	12	K	G	14	S	H	17	G	I	25	V	J	93	N	K	67	Q	L	28	C	M	70	Y	N	39	H	O	117	O	P	36	R	Q
31	B	F	56	T	G	62	I	H	102	Z	I	15	E	J	7	F	K	73	H	L	45	L	M	18	N	N	50	Q	O	123	Y	P	109	W	Q	4	M	R
106	Z	T	104	V	U	88	G	V	37	F	W	119	Y	X	34	D	Y	42	O	Z	59	E	A	20	S	B	81	X	C	92	Q	D	43	L	E	9	T	F
52	20 (5)	Q	76	1 (1)	R	48	7 (2)	S	120	2 (2)	T	16	16 (1)	U	33	12 (2)	V	54	18 (3)	W	114	6 (1)	X	79	22 (2)	Y	19	23 (3)	Z	44	9 (4)	A	105	24 (4)	B	115	5 (5)	C
3	L	S	30	R	T	72	R	U	22	R	V	1	R	W	101	L	X	130	R	Y	41	R	Z	11	R	A	24	R	B	85	R	C	80	L	D	94	L	E

N		E	O		O	P		E	Q		O	R		E	S		O	T		E	U		O	V		E	W		O		X	E	Y		O	Z		E
49	P	R	82	E	S	47	F	T	68	X	U	23	B	V	118	A	W	57	M	X	27	Z	Y	29	T	Z	77	I	A	60	D	B	127	J	C	6	U	D
75	P	S	64	S	T	10	K	U	63	X	V	83	U	W	129	C	X	2	V	Y	71	A	Z	87	O	A	112	G	B	61	R	C	116	D	D	108	J	E
74	K	G	103	H	H	86	P	I	89	B	J	38	M	K	122	J	L	46	W	M	66	T	N	69	A	O	111	C	P	26	R	Q	55	N	R	5	I	S
99	3 (3)	D	13	14 (4)	E	126	25 (5)	F	107	8 (3)	G	40	11 (1)	H	97	26 (1)	I	95	10 (5)	J	58	15 (5)	K	91	4 (4)	L	35	21 (1)	M	121	19 (4)	N	128	17 (2)	O	98	13 (3)	P
32	L	F	90	R	G	96	L	H	21	R	I	51	L	J	124	L	K	113	L	L	84	L	M	53	R	N	100	L	O	65	L	P	110	R	Q	78	L	R

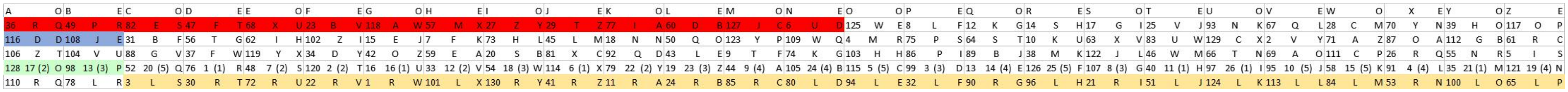
C-> (S)-> row 4-> shift right 2 spaces

N-> (O)-> row 5-> shift left 24 spaces

C-> (S)-> row 2-> shift right 2 spaces

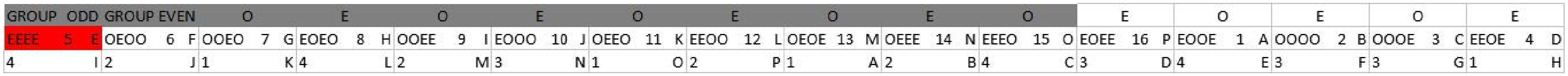
Q-> (E)-> row 1-> shift right 14 spaces

The **rows are the same** as referenced in the prior step. The Shifter field is shifted.



A O	B E	C O	D E	E O	F E	G O	H E	I O	J E	K O	L E	M O	N E	O O	P E	Q O	R E	S O	T E	U O	V E	W O	X E	Y O	Z E
36 R Q	49 P R	82 E S	47 F T	68 X U	23 B V	118 A W	57 M X	27 Z Y	29 T Z	77 I A	60 D B	127 J C	6 U D	125 W E	8 L F	12 K G	14 S H	17 G I	25 V J	93 N K	67 Q L	28 C M	70 Y N	39 H O	117 O P
116 D D	108 J E	31 B F	56 T G	62 I H	102 Z I	15 E J	7 F K	73 H L	45 L M	18 N N	50 Q O	123 Y P	109 W Q	4 M R	75 P S	64 S T	10 K U	63 X V	83 U W	129 C X	2 V Y	71 A Z	87 O A	112 G B	61 R C
106 Z T	104 V U	88 G V	37 F W	119 Y X	34 D Y	42 O Z	59 E A	20 S B	81 X C	92 Q D	43 L E	9 T F	74 K G	103 H H	86 P I	89 B J	38 M K	122 J L	46 W M	66 T N	69 A O	111 C P	26 R Q	55 N R	5 I S
128 17 (2) O	98 13 (3) P	52 20 (5) Q	76 1 (1) R	48 7 (2) S	120 2 (2) T	16 16 (1) U	33 12 (2) V	54 18 (3) W	114 6 (1) X	79 22 (2) Y	19 23 (3) Z	44 9 (4) A	105 24 (4) B	115 5 (5) C	99 3 (3) D	13 14 (4) E	126 25 (5) F	107 8 (3) G	40 11 (1) H	97 26 (1) I	95 10 (5) J	58 15 (5) K	91 4 (4) L	35 21 (1) M	121 19 (4) N
110 R Q	78 L R	3 L S	30 R T	72 R U	22 R V	1 R W	101 L X	130 R Y	41 R Z	11 R A	24 R B	85 R C	80 L D	94 L E	32 L F	90 R G	96 L H	21 R I	51 L J	124 L K	113 L L	84 L M	53 R N	100 L O	65 L P

We shift the Salt field EO seed row 1 space right.



GROUP ODD	GROUP EVEN	O	E	O	E	O	E	O	E	O	E	O	E	O	E
EEEE 5 E	OEOO 6 F	OOEO 7 G	EOEO 8 H	OOEE 9 I	EOOO 10 J	OEEO 11 K	EEOO 12 L	OEOE 13 M	OEEE 14 N	EEEO 15 O	EOEE 16 P	EOOE 1 A	OOOO 2 B	OOOE 3 C	EEOE 4 D
4 I	2 J	1 K	4 L	2 M	3 N	1 O	2 P	1 A	2 B	4 C	3 D	4 E	3 F	3 G	1 H

We assess for rule compliance with Pointer field pointer positions. **If no**, we execute the forcing rule.

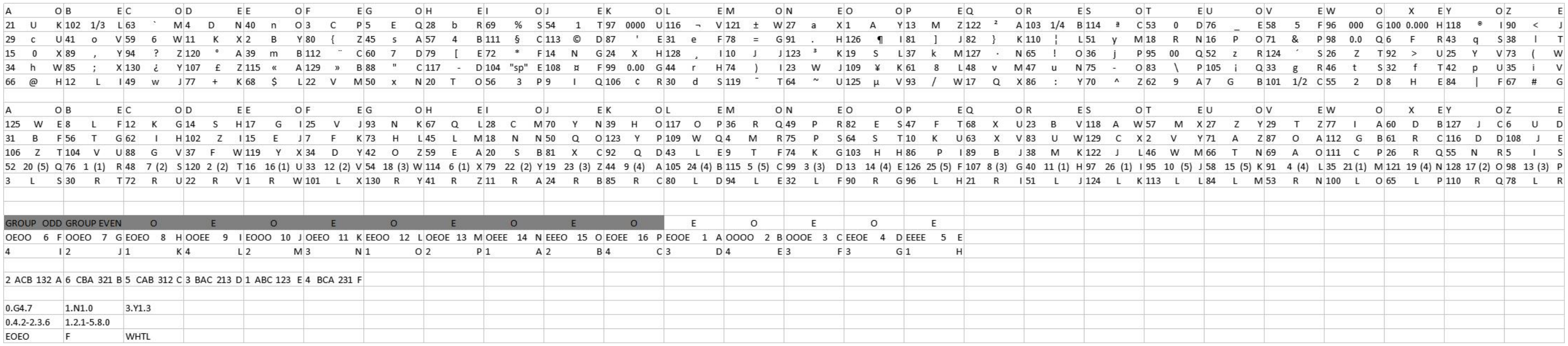
If yes, we continue and return to START 1 to re-begin steps for encrypting.

Once the final character is encrypted we return to START 1 to re-begin to assess for any Polyphasic salt and Phantom shift that would have occurred if more characters to encrypt remained. Once these are executed the encryption process is completed.

END

START 2

To decrypt a message we begin by performing the same initial setup as described above.



A O	B E	C O	D E	E O	F E	G O	H E	I O	J E	K O	L E	M O	N E	O O	P E	Q O	R E	S O	T E	U O	V E	W O	X E	Y O	Z E
21 U K	102 1/3 L	63 ` M	4 D N	40 n O	3 C P	5 E Q	28 b R	69 % S	54 1 T	97 0000 U	116 ¬ V	121 ± W	27 a X	1 A Y	13 M Z	122 ² A	103 1/4 B	114 ª C	53 0 D	76 _ E	58 5 F	96 000 G	100 0.000 H	118 ® I	90 < J
29 c U	41 o V	59 6 W	11 K X	2 B Y	80 { Z	45 s A	57 4 B	111 § C	113 © D	87 ' E	31 e F	78 = G	91 . H	126 ¶ I	81] J	82 } K	110 ¦ L	51 y M	18 R N	16 P O	71 & P	98 0.0 Q	6 F R	43 q S	38 l T
15 0 X	89 , Y	94 ? Z	120 ° A	39 m B	112 ¨ C	60 7 D	79 [E	72 * F	14 N G	24 X H	128 ¸ I	10 J J	123 ³ K	19 S L	37 k M	127 · N	65 ! O	36 j P	95 00 Q	52 z R	124 ´ S	26 Z T	92 > U	25 Y V	73 (W
34 h W	85 ; X	130 ¿ Y	107 £ Z	115 « A	129 » B	88 " C	117 - D	104 "sp" E	108 ¤ F	99 0.00 G	44 r H	74) I	23 W J	109 ¥ K	61 8 L	48 v M	47 u N	75 - O	83 \ P	105 ¡ Q	33 g R	46 t S	32 f T	42 p U	35 i V
66 @ H	12 L I	49 w J	77 + K	68 $ L	22 V M	50 x N	20 T O	56 3 P	9 I Q	106 ¢ R	30 d S	119 ¯ T	64 ~ U	125 µ V	93 / W	17 Q X	86 : Y	70 ^ Z	62 9 A	7 G B	101 1/2 C	55 2 D	8 H E	84 | F	67 # G
A O	B E	C O	D E	E O	F E	G O	H E	I O	J E	K O	L E	M O	N E	O O	P E	Q O	R E	S O	T E	U O	V E	W O	X E	Y O	Z E
125 W E	8 L F	12 K G	14 S H	17 G I	25 V J	93 N K	67 Q L	28 C M	70 Y N	39 H O	117 O P	36 R Q	49 P R	82 E S	47 F T	68 X U	23 B V	118 A W	57 M X	27 Z Y	29 T Z	77 I A	60 D B	127 J C	6 U D
31 B F	56 T G	62 I H	102 Z I	15 E J	7 F K	73 H L	45 L M	18 N N	50 Q O	123 Y P	109 W Q	4 M R	75 P S	64 S T	10 K U	63 X V	83 U W	129 C X	2 V Y	71 A Z	87 O A	112 G B	61 R C	116 D D	108 J E
106 Z T	104 V U	88 G V	37 F W	119 Y X	34 D Y	42 O Z	59 E A	20 S B	81 X C	92 Q D	43 L E	9 T F	74 K G	103 H H	86 P I	89 B J	38 M K	122 J L	46 W M	66 T N	69 A O	111 C P	26 R Q	55 N R	5 I S
52 20 (5) Q	76 1 (1) R	48 7 (2) S	120 2 (2) T	16 16 (1) U	33 12 (2) V	54 18 (3) W	114 6 (1) X	79 22 (2) Y	19 23 (3) Z	44 9 (4) A	105 24 (4) B	115 5 (5) C	99 3 (3) D	13 14 (4) E	126 25 (5) F	107 8 (3) G	40 11 (1) H	97 26 (1) I	95 10 (5) J	58 15 (5) K	91 4 (4) L	35 21 (1) M	121 19 (4) N	128 17 (2) O	98 13 (3) P
3 L S	30 R T	72 R U	22 R V	1 R W	101 L X	130 R Y	41 R Z	11 R A	24 R B	85 R C	80 L D	94 L E	32 L F	90 R G	96 L H	21 R I	51 L J	124 L K	113 L L	84 L M	53 R N	100 L O	65 L P	110 R Q	78 L R
GROUP ODD	GROUP EVEN	O	E	O	E	O	E	O	E	O	E	O	E	O	E										
OEOO 6 F	OOEO 7 G	EOEO 8 H	OOEE 9 I	EOOO 10 J	OEEO 11 K	EEOO 12 L	OEOE 13 M	OEEE 14 N	EEEO 15 O	EOEE 16 P	EOOE 1 A	OOOO 2 B	OOOE 3 C	EEOE 4 D	EEEE 5 E										
4 I	2 J	1 K	4 L	2 M	3 N	1 O	2 P	1 A	2 B	4 C	3 D	4 E	3 F	3 G	1 H										
2 ACB 132 A	6 CBA 321 B	5 CAB 312 C	3 BAC 213 D	1 ABC 123 E	4 BCA 231 F																				
0.G4.7	1.N1.0	3.Y1.3																							
0.4.2-2.3.6	1.2.1-5.8.0																								
EOEO	F	WHTL																							

We then assess the key for the first Polyphasic salt, first Phantom shift and then the seconds, thirds etc following the same steps as at the START of the encryption process. The difference is we will be passing the encrypted cipher text through the Enigma machine string in the **reverse order** it was passed to encrypt it. We will still follow the order in which the characters hold.

Polyphasic salt 0.G4.7/3.Y1.3/1.N1.0/

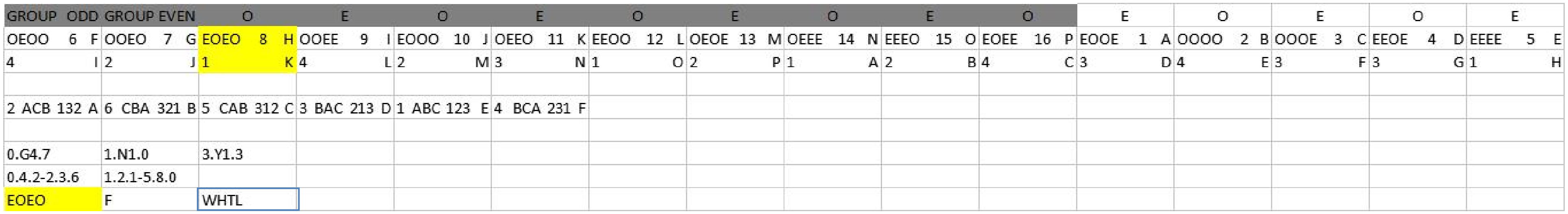
Path -> X A M L Z -> 4, 1, 3, 2, 5 -> Pass H through machines in Reverse order 4, 1, 3, 2, 5 = 5, 2, 3, 1, 4 -> Output E

Phantom shift 0.4.2.-2.3.6/1.2.1-5.8.0/

On step 0 (zero),on machine 4, counter 2, move forward 2 letters every after every 3rd character group, ending after the 6th occurance.

J -> K -> L

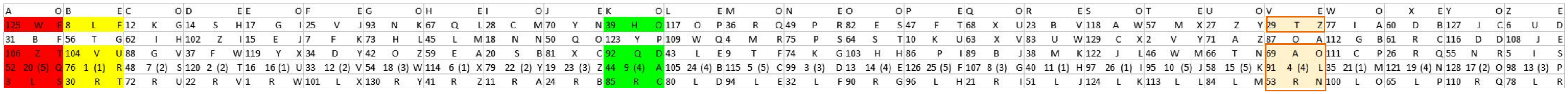
We then reference the EO seed to assess whether salt was active (was placed) to determine our target group length of 3 or 4. We also assess the placement of the potential salt.



GROUP ODD	GROUP EVEN	O	E	O	E	O	E	O	E	O	E	O	E	O	E
OEOO 6 F	OOEO 7 G	EOEO 8 H	OOEE 9 I	EOOO 10 J	OEEO 11 K	EEOO 12 L	OEOE 13 M	OEEE 14 N	EEEO 15 O	EOEE 16 P	EOOE 1 A	OOOO 2 B	OOOE 3 C	EEOE 4 D	EEEE 5 E
4 I	2 J	1 K	4 L	2 M	3 N	1 O	2 P	1 A	2 B	4 C	3 D	4 E	3 F	3 G	1 H
2 ACB 132 A	6 CBA 321 B	5 CAB 312 C	3 BAC 213 D	1 ABC 123 E	4 BCA 231 F										
0.G4.7	1.N1.0	3.Y1.3													
0.4.2-2.3.6	1.2.1-5.8.0														
EOEO	F	WHTL													

Salt is active, the target group length is 4 letters and the salt position is 1.

If yes, we reference the Height seed WHTL for the paths and reference each ciphertext path in the same manner as before.



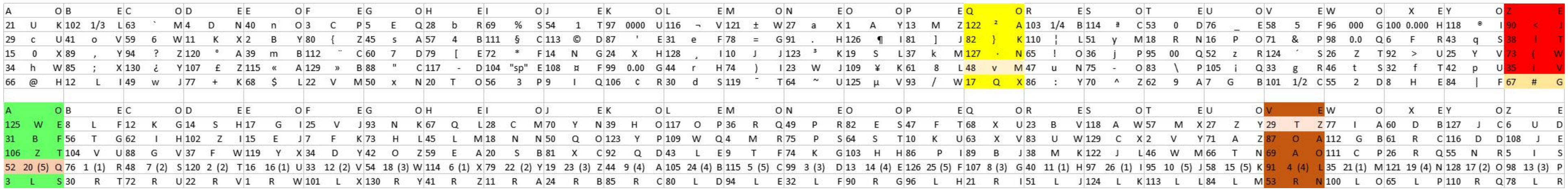
A O	B E	C O	D E	E O	F E	G O	H E	I O	J E	K O	L E	M O	N E	O O	P E	Q O	R E	S O	T E	U O	V E	W O	X E	Y O	Z E
125 W E	8 L F	12 K G	14 S H	17 G I	25 V J	93 N K	67 Q L	28 C M	70 Y N	39 H O	117 O P	36 R Q	49 P R	82 E S	47 F T	68 X U	23 B V	118 A W	57 M X	27 Z Y	29 T Z	77 I A	60 D B	127 J C	6 U D
31 B F	56 T G	62 I H	102 Z I	15 E J	7 F K	73 H L	45 L M	18 N N	50 Q O	123 Y P	109 W Q	4 M R	75 P S	64 S T	10 K U	63 X V	83 U W	129 C X	2 V Y	71 A Z	87 O A	112 G B	61 R C	116 D D	108 J E
106 Z T	104 V U	88 G V	37 F W	119 Y X	34 D Y	42 O Z	59 E A	20 S B	81 X C	92 Q D	43 L E	9 T F	74 K G	103 H H	86 P I	89 B J	38 M K	122 J L	46 W M	66 T N	69 A O	111 C P	26 R Q	55 N R	5 I S
52 20 (5) Q	76 1 (1) R	48 7 (2) S	120 2 (2) T	16 16 (1) U	33 12 (2) V	54 18 (3) W	114 6 (1) X	79 22 (2) Y	19 23 (3) Z	44 9 (4) A	105 24 (4) B	115 5 (5) C	99 3 (3) D	13 14 (4) E	126 25 (5) F	107 8 (3) G	40 11 (1) H	97 26 (1) I	95 10 (5) J	58 15 (5) K	91 4 (4) L	35 21 (1) M	121 19 (4) N	128 17 (2) O	98 13 (3) P
3 L S	30 R T	72 R U	22 R V	1 R W	101 L X	130 R Y	41 R Z	11 R A	24 R B	85 R C	80 L D	94 L E	32 L F	90 R G	96 L H	21 R I	51 L J	124 L K	113 L L	84 L M	53 R N	100 L O	65 L P	110 R Q	78 L R

1) W -> Odd(pointer field), column Z, Even(letters) row 5, down -> G J T W V -> 1, 2, 3, 5, 4

2) H-> Odd(pointer field), column Q, Odd(numbers) row 4, up -> 48, 127, 82, 122, 17 -> 2, 5, 3, 4, 1

3) T-> Even(shifter field), column A, Even(letters) row 4, up -> Q, T, F, E, S -> 3, 5, 2, 1, 4

4) L-> Even(shifter field), column V, Odd(numbers) row 1, up -> 29, 53, 91, 89, 87 -> 1, 2, 5, 4, 3



A O	B E	C O	D E	E O	F E	G O	H E	I O	J E	K O	L E	M O	N E	O O	P E	Q O	R E	S O	T E	U O	V E	W O	X E	Y O	Z E
21 U K	102 1/3 L	63 ` M	4 D N	40 n O	3 C P	5 E Q	28 b R	69 % S	54 1 T	97 0000 U	116 ¬ V	121 ± W	27 a X	1 A Y	13 M Z	122 ² A	103 1/4 B	114 ª C	53 0 D	76 _ E	58 5 F	96 000 G	100 0.000 H	118 ® I	90 < J
29 c U	41 o V	59 6 W	11 K X	2 B Y	80 { Z	45 s A	57 4 B	111 § C	113 © D	87 ' E	31 e F	78 = G	91 . H	126 ¶ I	81] J	82 } K	110 ¦ L	51 y M	18 R N	16 P O	71 & P	98 0.0 Q	6 F R	43 q S	38 I T
15 0 X	89 , Y	94 ? Z	120 ° A	39 m B	112 ¨ C	60 7 D	79 [E	72 * F	14 N G	24 X H	128 ¸ I	10 J J	123 ³ K	19 S L	37 k M	127 · N	65 ! O	36 j P	95 00 Q	52 z R	124 ´ S	26 Z T	92 > U	25 Y V	73 (W
34 h W	85 ; X	130 ¿ Y	107 £ Z	115 « A	129 » B	88 " C	117 - D	104 "sp" E	108 ¤ F	99 0.00 G	44 r H	74) I	23 W J	109 ¥ K	61 8 L	48 v M	47 u N	75 - O	83 \ P	105 ¡ Q	33 g R	46 t S	32 f T	42 p U	35 i V
66 @ H	12 L I	49 w J	77 + K	68 $ L	22 V M	50 x N	20 T O	56 3 P	9 I Q	106 ¢ R	30 d S	119 ¯ T	64 ~ U	125 µ V	93 / W	17 Q X	86 : Y	70 ^ Z	62 9 A	7 G B	101 1/2 C	55 2 D	8 H E	84 | F	67 # G

A O	B E	C O	D E	E O	F E	G O	H E	I O	J E	K O	L E	M O	N E	O O	P E	Q O	R E	S O	T E	U O	V E	W O	X E	Y O	Z E
125 W E	8 L F	12 K G	14 S H	17 G I	25 V J	93 N K	67 Q L	28 C M	70 Y N	39 H O	117 O P	36 R Q	49 P R	82 E S	47 F T	68 X U	23 B V	118 A W	57 M X	27 Z Y	29 T Z	77 I A	60 D B	127 J C	6 U D
31 B F	56 T G	62 I H	102 Z I	15 E J	7 F K	73 H L	45 L M	18 N N	50 Q O	123 Y P	109 W Q	4 M R	75 P S	64 S T	10 K U	63 X V	83 U W	129 C X	2 V Y	71 A Z	87 O A	112 G B	61 R C	116 D D	108 J E
106 Z T	104 V U	88 G V	37 F W	119 Y X	34 D Y	42 O Z	59 E A	20 S B	81 X C	92 Q D	43 L E	9 T F	74 K G	103 H H	86 P I	89 B J	38 M K	122 J L	46 W M	66 T N	69 A O	111 C P	26 R Q	55 N R	5 I S
52 20 (5) Q	76 1 (1) R	48 7 (2) S	120 2 (2) T	16 16 (1) U	33 12 (2) V	54 18 (3) W	114 6 (1) X	79 22 (2) Y	19 23 (3) Z	44 9 (4) A	105 24 (4) B	115 5 (5) C	99 3 (3) D	13 14 (4) E	126 25 (5) F	107 8 (3) G	40 11 (1) H	97 26 (1) I	95 10 (5) J	58 15 (5) K	91 4 (4) L	35 21 (1) M	121 19 (4) N	128 17 (2) O	98 13 (3) P
3 L S	30 R T	72 R U	22 R V	1 R W	101 L X	130 R Y	41 R Z	11 R A	24 R B	85 R C	80 L D	94 L E	32 L F	90 R G	96 L H	21 R I	51 L J	124 L K	113 L L	84 L M	53 R N	100 L O	65 L P	110 R Q	78 L R

We then pass the cipher text through the path in the **reverse order** with which it was encrypted.

1) W -> Odd(pointer field), column Z, Even(letters) row 5, down -> G J T W V -> 1, 2, 3, 5, 4 -> pass D through 4, 5, 3, 2, 1-> Output C

2) H-> Odd(pointer field), column Q, Odd(numbers) row 4, up -> 48, 127, 82, 122, 17 -> 2, 5, 3, 4, 1-> pass R through 1, 4, 3, 5, 2-> Output N

3) T-> Even(shifter field), column A, Even(letters) row 4, up -> Q, T, F, E, S -> 3, 5, 2, 1, 4-> pass Z through 4, 1, 2, 5, 3-> Output C

4) L-> Even(shifter field), column V, Odd(numbers) row 1, up -> 29, 53, 91, 89, 87 -> 1, 2, 5, 4, 3-> pass C through 3, 4, 5, 2, 1-> Output Q

We then save this set CNCQ for future reference of a new EO seed, height seed and shift functions.

The salt is removed and the Slider seed is referenced and **reversed** to return to ABC 123. C N C Q-> NCQ (N C Q = BCA -> Q N C = ABC)

2 ACB 132 A	6 CBA 321 B	5 CAB 312 C	3 BAC 213 D	1 ABC 123 E	4 BCA 231 F
0.G4.7	1.N1.0	3.Y1.3			
0.4.2-2.3.6	1.2.1-5.8.0				
EOEO	F	WHTL			

The pointer set can now be correlated to the Target character.

A		O	B		E	C		O	D		E	E		O	F		E	G		O	H		E	I		O
21	U	K	102	1/3	L	63	`	M	4	D	N	40	n	O	3	C	P	5	E	Q	28	b	R	69	%	S
29	c	U	41	o	V	59	6	W	11	K	X	2	B	Y	80	{	Z	45	s	A	57	4	B	111	§	C
15	0	X	89	,	Y	94	?	Z	120	°	A	39	m	B	112	¨	C	60	7	D	79	[	E	72	*	F
34	h	W	85	;	X	130	¿	Y	107	£	Z	115	«	A	129	»	B	88	"	C	117	-	D	104	"sp"	E
66	@	H	12	L	I	49	w	J	77	+	K	68	$	L	22	V	M	50	x	N	20	T	O	56	3	P

J		E	K		O	L		E	M		O	N		E	O		O	P		E	Q		O	R		E
54	1	T	97	0000	U	116	¬	V	121	±	W	27	a	X	1	A	Y	13	M	Z	122	²	A	103	1/4	B
113	©	D	87	'	E	31	e	F	78	=	G	91	.	H	126	¶	I	81	]	J	82	}	K	110	¦	L
14	N	G	24	X	H	128	¸	I	10	J	J	123	³	K	19	S	L	37	k	M	127	·	N	65	!	O
108	¤	F	99	0.00	G	44	r	H	74	)	I	23	W	J	109	¥	K	61	8	L	48	v	M	47	u	N
9	I	Q	106	¢	R	30	d	S	119	¯	T	64	~	U	125	µ	V	93	/	W	17	Q	X	86	:	Y

S		O	T		E	U		O	V		E	W		O		X	E	Y		O	Z		E
114	ª	C	53	0	D	76	_	E	58	5	F	96	000	G	100	0.000	H	118	®	I	90	<	J
51	y	M	18	R	N	16	P	O	71	&	P	98	0.0	Q	6	F	R	43	q	S	38	l	T
36	j	P	95	00	Q	52	z	R	124	´	S	26	Z	T	92	>	U	25	Y	V	73	(	W
75	-	O	83	\	P	105	¡	Q	33	g	R	46	t	S	32	f	T	42	p	U	35	i	V
70	^	Z	62	9	A	7	G	B	101	1/2	C	55	2	D	8	H	E	84	|	F	67	#	G

If no, we assess the EO seed for the "would be"placement, assess the height seed for the paths and reference each cipher text path that were used omitting the salt path.

Since salt was position 1 we would omit the path designated by the first letter in the height seed WHTL as it did not pass through final encryption. We then pass each letter through the path in the **reverse** order with which it was encrypted.

1) W-> Odd(pointer field), column Z, Even(letters) row 5, down -> G J T W V -> 1, 2, 3, 5, 4 -> pass D through 4, 5, 3, 2, 1-> Output C

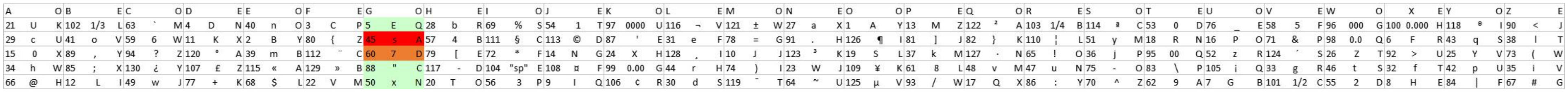
2) H-> Odd(pointer field), column Q, Odd(numbers) row 4, up -> 48, 127, 82, 122, 17 -> 2, 5, 3, 4, 1-> pass R through 1, 4, 3, 5, 2-> Output N

3) T-> Even(shifter field), column A, Even(letters) row 4, up -> Q, T, F, E, S -> 3, 5, 2, 1, 4-> pass Z through 4, 1, 2, 5, 3-> Output C

4) L-> Even(shifter field), column V, Odd(numbers) row 1, up -> 29, 53, 91, 89, 87 -> 1, 2, 5, 4, 3-> pass C through 3, 4, 5, 2, 1-> Output Q

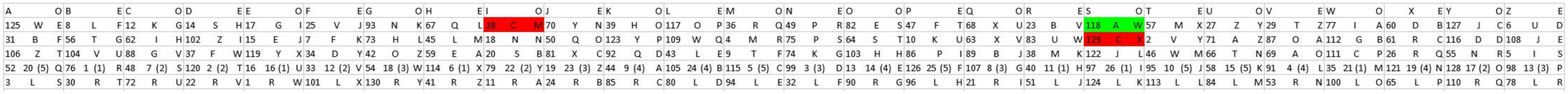
We reference the Slider seed and execute a **reverse** function. (N C Q = BCA ->Q N C = ABC)

We now correlate the pointer set to the Target character. We assess the omitted salt value A,



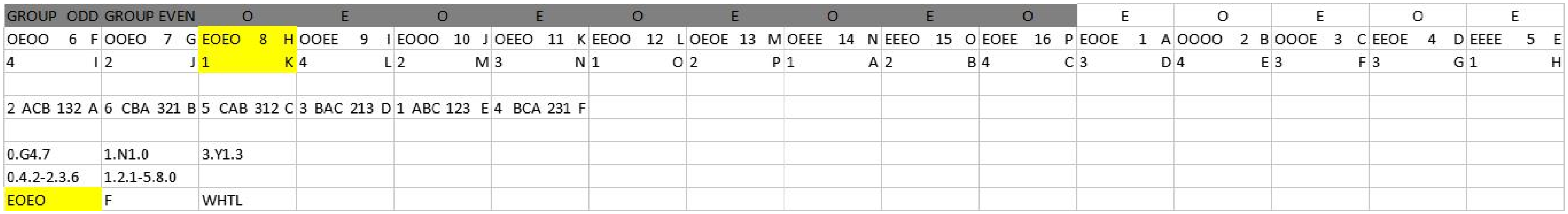
A		O	B		E	C		O	D		E	E		O	F		E	G		O	H		E	I		O	J		E	K		O	L		E	M		O	N		E	O		O	P		E	Q		O	R		E	S		O	T		E	U		O	V		E	W		O		X	E	Y		O	Z		E
21	U	K	102	1/3	L	63	`	M	4	D	N	40	n	O	3	C	P	5	E	Q	28	b	R	69	%	S	54	1	T	97	0000	U	116	¬	V	121	±	W	27	a	X	1	A	Y	13	M	Z	122	²	A	103	1/4	B	114	ª	C	53	0	D	76	_	E	58	5	F	96	000	G	100	0.000	H	118	®	I	90	<	J
29	c	U	41	o	V	59	6	W	11	K	X	2	B	Y	80	{	Z	45	s	A	57	4	B	111	§	C	113	©	D	87	'	E	31	e	F	78	=	G	91	.	H	126	¶	I	81	]	J	82	}	K	110	¦	L	51	y	M	18	R	N	16	P	O	71	&	P	98	0.0	Q	6	F	R	43	q	S	38	l	T
15	0	X	89	,	Y	94	?	Z	120	°	A	39	m	B	112	¨	C	60	7	D	79	[	E	72	*	F	14	N	G	24	X	H	128	¸	I	10	J	J	123	³	K	19	S	L	37	k	M	127	·	N	65	!	O	36	j	P	95	00	Q	52	z	R	124	´	S	26	Z	T	92	>	U	25	Y	V	73	(	W
34	h	W	85	;	X	130	¿	Y	107	£	Z	115	«	A	129	»	B	88	"	C	117	-	D	104	"sp"	E	108	¤	F	99	0.00	G	44	r	H	74	)	I	23	W	J	109	¥	K	61	8	L	48	v	M	47	u	N	75	-	O	83	\	P	105	¡	Q	33	g	R	46	t	S	32	f	T	42	p	U	35	i	V
66	@	H	12	L	I	49	w	J	77	+	K	68	$	L	22	V	M	50	x	N	20	T	O	56	3	P	9	I	Q	106	¢	R	30	d	S	119	¯	T	64	~	U	125	µ	V	93	/	W	17	Q	X	86	:	Y	70	^	Z	62	9	A	7	G	B	101	1/2	C	55	2	D	8	H	E	84	|	F	67	#	G

find its conversion C



A		O	B		E	C		O	D		E	E		O	F		E	G		O	H		E	I		O	J		E	K		O	L		E	M		O	N		E	O		O	P		E	Q		O	R		E	S		O	T		E	U		O	V		E	W		O		X	E	Y		O	Z		E
125	W	E	8	L	F	12	K	G	14	S	H	17	G	I	25	V	J	93	N	K	67	Q	L	28	C	M	70	Y	N	39	H	O	117	O	P	36	R	Q	49	P	R	82	E	S	47	F	T	68	X	U	23	B	V	118	A	W	57	M	X	27	Z	Y	29	T	Z	77	I	A	60	D	B	127	J	C	6	U	D
31	B	F	56	T	G	62	I	H	102	Z	I	15	E	J	7	F	K	73	H	L	45	L	M	18	N	N	50	Q	O	123	Y	P	109	W	Q	4	M	R	75	P	S	64	S	T	10	K	U	63	X	V	83	U	W	129	C	X	2	V	Y	71	A	Z	87	O	A	112	G	B	61	R	C	116	D	D	108	J	E
106	Z	T	104	V	U	88	G	V	37	F	W	119	Y	X	34	D	Y	42	O	Z	59	E	A	20	S	B	81	X	C	92	Q	D	43	L	E	9	T	F	74	K	G	103	H	H	86	P	I	89	B	J	38	M	K	122	J	L	46	W	M	66	T	N	69	A	O	111	C	P	26	R	Q	55	N	R	5	I	S
52	20 (5)	Q	76	1 (1)	R	48	7 (2)	S	120	2 (2)	T	16	16 (1)	U	33	12 (2)	V	54	18 (3)	W	114	6 (1)	X	79	22 (2)	Y	19	23 (3)	Z	44	9 (4)	A	105	24 (4)	B	115	5 (5)	C	99	3 (3)	D	13	14 (4)	E	126	25 (5)	F	107	8 (3)	G	40	11 (1)	H	97	26 (1)	I	95	10 (5)	J	58	15 (5)	K	91	4 (4)	L	35	21 (1)	M	121	19 (4)	N	128	17 (2)	O	98	13 (3)	P
3	L	S	30	R	T	72	R	U	22	R	V	1	R	W	101	L	X	130	R	Y	41	R	Z	11	R	A	24	R	B	85	R	C	80	L	D	94	L	E	32	L	F	90	R	G	96	L	H	21	R	I	51	L	J	124	L	K	113	L	L	84	L	M	53	R	N	100	L	O	65	L	P	110	R	Q	78	L	R

and impose into the **pre-reversed** pointer set by referencing the EO seed for position-> C N C Q



GROUP ODD	GROUP EVEN	O	E	O	E	O	E	O	E	O	E	O	E	O	E
OEOO 6 F	OOEO 7 G	EOEO 8 H	OOEE 9 I	EOOO 10 J	OEEO 11 K	EEOO 12 L	OEOE 13 M	OEEE 14 N	EEEO 15 O	EOEE 16 P	EOOE 1 A	OOOO 2 B	OOOE 3 C	EEOE 4 D	EEEE 5 E
4 I	2 J	1 K	4 L	2 M	3 N	1 O	2 P	1 A	2 B	4 C	3 D	4 E	3 F	3 G	1 H
2 ACB 132 A	6 CBA 321 B	5 CAB 312 C	3 BAC 213 D	1 ABC 123 E	4 BCA 231 F										
0.G4.7	1.N1.0	3.Y1.3													
0.4.2-2.3.6	1.2.1-5.8.0														
EOEO	F	WHTL													

We can now reference a new EO seed, height seed and shift functions.

We then assess the shift values for the Pointer field, Shifter field and Salt field and shift in the same manner as above. We then return to Start 2 to re-begin and continue.

END 2